NexSentry Manager Installation and Administrator's Guide

Limited Warranty

Westinghouse Security Electronics warrants to the original user the Equipment manufactured by Security Electronics as described herein (the Equipment) to be free from defects in material and workmanship for a period of **ninety days (90)** days from the date of purchase provided:

I Security Electronics has been notified within such period by return of any allleged defective equipment, free and clear of any liens and encumbrances to Security Electronics or its authorized Dealer at the address specified, transportation prepaid; and

II the Equipment has not been abused, misused or improperly maintained and/or repaired during such period; and

III such defect has not been caused by ordinary wear and tear; and

IV such defect is not a result of voltage surges/brownouts, lightning, water damage/flooding, fire, explosion, earthquakes, tornadoes, acts of aggression/war or similar phenomena; and

V accessories used as an integral to Security Electronics Systems have been approved by Security Electronics (e.g., coaxial cables, batteries, etc.); and

VI the Equipment has been installed, the installation supervised or installation tested by an authorized Security Electronics Dealer.

This guide contains proprietary information of Westinghouse Security Electronics and its receipt or possession does not convey any rights to reproduce, disclose its contents, or to manufacture, use or sell anything it may dscribe. Reproduction, disclosure or use without specific written authorization of Westinghouse Security Electronics is strictly forbidden.

RESTRICTED RIGHTS LEGEND Use, duplication, or disclosure by the Government is subject to restrictions as set forth in the subdivision (c)(1)(ii) of the Rights in Technical Data and Computer Software clause at DFARS 252.227-7013.

Westinghouse Security Electronics
5452 Betsy Ross Drive, Santa Clara, CA 95054-1184, USA.

© 1997 Westinghouse Security Electronics.

All rights reserved. Printed in the United States of America.

NexSentry™ is a trademark of Westinghouse Security Electronics.

Microsoft Windows NT® is a registered trademark of Microsoft Corporation.

TABLE OF CONTENTS

Preface

Welcome to NexSentry Manager vii
Understanding Access Control vii
NexSentry Manager Features vii
Using this Guide ix

Chapter 1
Getting Started

Chapter Overview 1-1
Key Terms 1-1
Before You Begin 1-2
Assumptions 1-2
System Requirements 1-2
Initial Setup Process 1-3
Installing the Software 1-4
Software Installation Overview 1-4
Installing the Software 1-4
Testing the System 1-6
Touring the NexSentry Manager 1-9
Using Online Help 1-10
Planning the Database 1-11
Gathering Data 1-11
Completing the Input Forms 1-12
Using the Database 1-13
Browsing the Database 1-13
Sort and Filter 1-16

Chapter 2
System Administration Data

Chapter Overview 2-1
Key Terms 2-1
About System Admin 2-2

Using System Admin Screens 2-3
Security Levels 2-4
System Users 2-6
ACU Users 2-8
Transactions 2-10
Alarm Responses 2-12
Audit Trail 2-13
User Defined Fields 2-14
Facility Codes 2-16
Miscellaneous 2-17
Time Codes 2-17
Time Groups 2-19
Holidays 2-20
Actions 2-21
Action Groups 2-23
Maps 2-25
Sounds 2-26
System Defaults 2-27

Chapter 3
Hardware and Facility Data

Chapter Overview 3-1
Key Terms.....3-1
Using Hardware Screens 3-2
Pollers 3-3
Entering Data 3-3
Access Control Units (ACU) 3-5
Addressing ACUs.....3-5
Entering ACU Data.....3-7
Doors 3-9
Entering Door Data 3-9
Inputs 3-11
Outputs 3-13
Instructions 3-15
Zones 3-16

Maps 3-17

Chapter 4
Cardholder Data

Chapter Overview 4-1
Key Terms.....4-1
Configuring Access Codes 4-2
Configuring Cardholders 4-4

Chapter 5
Using NexSentry Manager

Chapter Overview 5-1
Key Terms.....5-1
Monitoring Current Transactions 5-2
Using the Monitor Window 5-2
The Monitor Menu.....5-3
Viewing Recent Transactions 5-3
Sorting Transactions.....5-3
Viewing the Transaction Log 5-5
Changing Transaction Defaults.....5-5
Archiving.....5-6
Working With Alarms 5-8
Viewing Alarms 5-8
Acknowledging and Silencing Alarms.....5-8
Checking System Status 5-10
Viewing Status Windows.....5-10
Filtering Status Window Data.....5-10
Activating the Status Menu.....5-10
Using Maps 5-14
Backing Up the System 5-15

Chapter 6
Troubleshooting

Chapter Overview 6-1
Key Terms.....6-1
Error Messages 6-5

Appendix A

NexSentry Manager Input Forms

Appendix B

NexSentry Manager Database File Structure

Glossary

Index

Preface

Welcome to NexSentry Manager

Understanding Access Control

The simplest form of access control is a lock and key, without which a door cannot be opened. Electronic access control and alarm monitoring systems provide much more than this.

Electronic access control systems like NexSentry Manager use complex electrical, electronic, and computer technology to determine who has access permission, where and when permission is granted, and to monitor and record all events, both the ordinary and the extraordinary. The system monitors vulnerable places for danger and its own components for failure or tampering.

NexSentry Manager Features

NexSentry Manager allows operators to be aware of and control:

- Entry and exit of up to 50,000 people through up to 256 doors.
- Consequences of nearly 200 types of events.
- Sufficient configurations of ACUs, sensors, monitors, door locks, and other access devices (limit is determined by the number of ACUs on your system).
- Where and why someone is being denied access through a door.
- Which doors are automatically being unlocked.
- Where a door is being held open too long.
- Who has entered a particular door and when.
- Which monitor point has been activated.
- Where power has gone out or has been restored.
- Which control devices are working and which are not.

The NexSentry Manager system provides control for:

- Multiple access devices, such as proximity sensors, magnetic stripe readers, and keypads that screen people at doors, turnstiles, and parking lot gates.
- Multiple monitor devices that can observe infrared and microwave intrusion detectors, dampness levels, and window and door contacts.
- Relay output contacts that can sound alarms, unlock doors, turn on video cameras, air conditioning, lights, and notify police and fire departments.
- Custom programming of ACUs and alarm monitoring systems.
- User-defined operator instructions linked to individual events.
- Report-generating capability to trace cardholders, monitor door use, oversee operator activity, and system event history.
- Event data Filtering and Sorting.
- Backup with any routine you desire.

Using this Guide

This guide is directed to the system users of the NexSentry Manager. It is organized to logically take you through the software installation and initial configuration process and on to the day-to-day activities involved in managing the system.

- **Chapter 1, Getting Started** describes the initial software installation and gives you an overview of the processes of configuring the system and using it on a day-to-day basis.
- **Chapter 2, System Administration Data** covers the viewing, editing and configuring of the data for customizing and controlling access to the system.
- **Chapter 3, Hardware and Facility Data** helps you to begin entering the hardware and facility data. This is how you tell the NexSentry Manager which devices you have installed within the system.
- **Chapter 4, Cardholder Data** covers how and when cardholders will be able to have access to the building.
- **Chapter 5, Using the Database** helps with the daily tasks of monitoring and maintaining the database.
- **Chapter 6, Troubleshooting** helps you in case you run into problems or errors when setting-up and using the NexSentry Manager software.
- **The Glossary** defines some of the unique terminology necessary to use the NexSentry system.
- **The Index** provides a quick way to find the information you are seeking.
- **Appendices** provide the NexSentry Manager Input Forms and detailed information on the database structure.

Chapter 1
Getting Started

Chapter Overview

This chapter explains the basics of the NexSentry Manager, and helps you get the system up and running.

- Before You Begin Page 1-2
- Initial Setup Process Page 1-3
- Installing the Software Page 1-4
- Testing the System Page 1-6
- Touring the NexSentry Manager Page 1-9
- Using Online Help Page 1-10
- Planning the Database Page 1-11
- Using the Database Page 1-13

Key Terms

- **System Administrator Data:** *The information about who will monitor, view and input data in the NexSentry Manager.*
- **Hardware or Facility Data:** *All of the information about the facility and the security equipment installed from ACU's to types of cards used. This information will come from the installer.*
- **Cardholder Data:** *The information about the people accessing the building. This includes personal data as well as where and when they have access.*
- **Access Control Units (ACUs):** *The devices which sense and react to inputs from the secured environment.*
- **Pollers:** *The system elements which control actual communications with devices. There is only one poller for each communications port (for example, Poller1=COM1, Poller2=COM2).*

Before You Begin

Assumptions

This guide assumes that the installer has completed all security system hardware installation, and therefore does not deal with the installation of the hardware. This guide begins with the gathering and entering of your particular site information and concludes with the basic day-to-day operation.

Secondly, this guide assumes that the Windows NT operating system is up and running on the NexSentry host computer. This guide also assumes that you have a basic understanding of Windows NT, or at least an understanding of the way Windows programs operate. If you are not familiar with Windows, then take a few minutes to browse through the online Help or other orientation information. With a basic understanding of Windows, using NexSentry Manager is easy to learn.

Finally, this guide and the software assume that your computer system meets the appropriate system requirements, listed below.

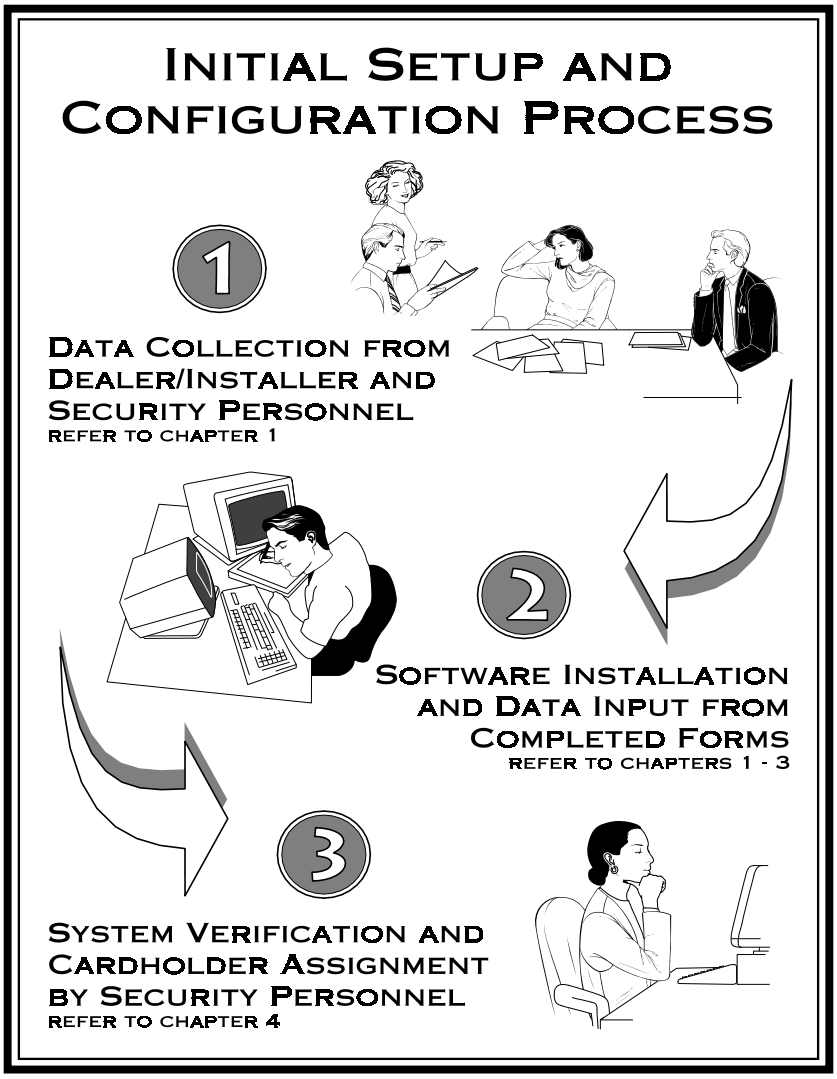
System Requirements

The NexSentry Manager System requirements:

- IBM Compatible Pentium with a minimum of 32 MB of RAM
- Microsoft Windows NT 4.0 or later
- 540 MB of free hard disk space
- SVGA Video
- 3.5 inch, 1.4 MB Floppy Drive
- Three or more RS-232 serial ports available
- CD-ROM drive
- Tape backup drive (recommended but optional)

Initial Setup Process

The following graphic shows the overall process to get your NexSentry system up and running.


INITIAL SETUP AND CONFIGURATION PROCESS
1
DATA COLLECTION FROM DEALER/INSTALLER AND SECURITY PERSONNEL
REFER TO CHAPTER 1
2
SOFTWARE INSTALLATION AND DATA INPUT FROM COMPLETED FORMS
REFER TO CHAPTERS 1 - 3
3
SYSTEM VERIFICATION AND CARDHOLDER ASSIGNMENT BY SECURITY PERSONNEL
REFER TO CHAPTER 4

Installing the Software

Software Installation Overview

The CD in your package includes an installation program to help you quickly install your copy of the NexSentry Manager. The installer prompts you through the entire process.

Note

You cannot install the NexSentry Manager just by copying the files to your hard disk because many of the files are compressed, and the installer needs to make entries in Windows configuration files.

Installing the Software

1. Locate your CD and insert in the CD-ROM drive.
2. The autostart file will begin the installation. If your autostart setting is disabled, then:

   a. Choose **Run** from the Start Menu.

   b. Type **`d:\setup`** in the box and click **OK**.

Note

This assumes drive "d" is a CD-ROM. If you are installing from another drive, substitute the letter for that drive instead.

If you get prompts during the installation program and you are unsure of the correct response, contact your installer for the correct information.

3. Follow the instructions of the installation program.

Tip

You will be asked several questions during the installation. Up to date information is available by reading the Release Notes that appears in the NexSentry Manager program directory.

Here are a few more tips:

If you are using a Microsoft TCP/IP Network, you must know the IP address of the computer that will be used as the server as well as the addresses of any other computers that will be using just the client.

You will receive a message the following message during the installation:

Information
Install will now start the WHC driver Utility. If the next window reads 'create driver registry entries...', please choose yes. If the next window reads 'Winstar WHC Utility...', please click exit.
OK

*This installation program behaves differently depending on if this is a new install or a re-install. If this is a new install you will be asked to confirm the installation of the drivers. Click **OK** when asked if you want to install the driver. If this is a reinstall then a small window will pop-up indicating the driver is already present. Click **Exit** to continue.*

4. When installation is complete, the computer will need to reboot. If the computer appears to lock-up, power off the computer, wait three seconds, then power on the computer (or press the reset button on the front). After Windows NT re-starts, the NexSentry Group will be open. Double-click the NexSentry Client.
5. When the Main window appears, you can begin data entry as described later in this chapter. To do this, log on the system by entering the default log on name,

   `Administrator`

   Press Enter, type the default password,

   `new123`

   and press Enter again.

Note

Because you have not configured the software to your site, the NexSentry Manager is not ready to operate. The real work is about to begin!

Testing the System

After installation, you should test the NexSentry Manager before you begin entering all of your data. The Database contains all of the information you need to test the system. Use the procedures below to test your system. The testing procedures are the same as those that you will use to input all of the information about your system.

Tip

Your installer may have already performed a system test. You may want to check with the installer before proceeding.

Addressing your first ACU:

This first step requires the use of a terminal emulation program, such as the Windows NT Hyperterminal. Configure Hyperterminal to use the following settings:

- Connect using: COM1
- Bits per second (Baud Rate): 9600
- Data Bits: 7
- Parity: Odd
- Stop bits:1
- Flow control: None

Tip

Save this setting to use for later configuration of other ACUs

Make sure that you are connected to the correct Serial Port on your computer and that you are also connected with the Terminal Port on the ACU before testing the system.

Once you have configured the COM settings in Hyperterminal, perform the following to address and configure ACUs:

1. Run Hyperterminal.
2. Select **Connect** to communicate with the ACU and then press the space bar. The ACU will respond: **"Password?"**
3. Type the Default password**: NEW** and press **Enter**.
4. You will be logged in and receive another prompt: "**Your command?"**
5. Type **SYS** and press **Enter.**
6. Now press **Enter** several times until you reach the prompt: **"Address."**
7. Enter "**1**"

8. If the ACU is running at a baud rate of less than **9600**, you can change that setting now as well. Type **SYS** and press Enter several times until you read **Host Baud**. Type **9600** and press **Enter**. Type **9600** into **Terminal Baud** and press **Enter** again**.**
9. When you are finished Addressing the ACU, press the **Escape** key, type **Reset** and press **Enter**. This will save the changes you have made and reset the ACU to be able to connect with NexSentry Manager. If you have changed the baud rate, reset will immediately change the baud rate to the one you set. If you still have to communicate directly, you will have to reconfigure your terminal program to use the new baud rate setting.

Tip

If you have made a mistake addressing an ACU, return to it and do the previous steps, making corrections as necessary.

Configure Hardware in the NexSentry Manager

1. Run the NexSentry Manager by clicking on the NexSentry Manager icon.

NexSentry Manager

2. Click on the Status Tool to display the Status dialog box.
3. Select ACU and click OK.

This window will show you if the ACU that you just addressed is online.

Status Tool

If the ACU is working properly, you should see a lightning bolt symbol in the Communications column.

If the ACU is not working properly, see "Troubleshooting," Page 6-1 or contact your installer.

Reading Your First Card

From the Main Menu:

1. Choose Database, Add and then Cardholder. This will bring up the Add/Edit Cardholder Dialog Box.
2. Enter the Cardholder information for one of the entries on your Cardholder list or yourself. It is important to fill out the General, Access and Credentials pages of this dialog box at this time. For the Credentials, select an access card and enter the number from that card.
3. When you have finished entering, click OK.

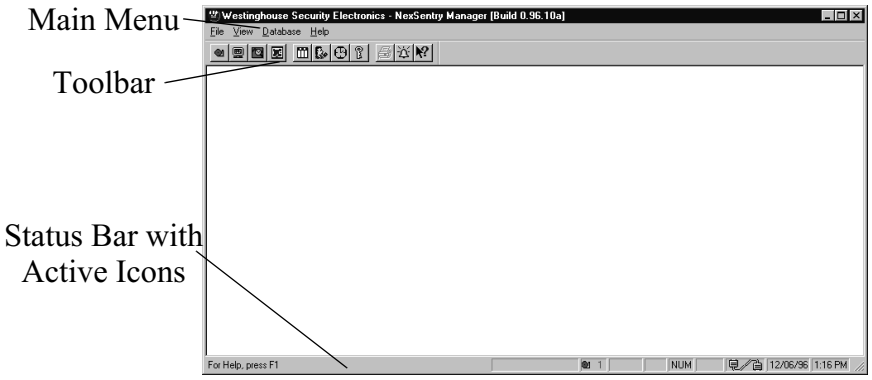
4. Finally, try using the card you just configured. Find the digital card reader that is associated with ACU 1 and test the card.

   If the Digital Card Reader is working, you will see the Reader light turn to green and also see Access Granted in the Monitor window.

   If the ACU or the Digital Card Reader is not working properly, see "Troubleshooting," Page 6-1 or contact your installer.

Touring the NexSentry Manager

At this point, you have successfully installed the software and are now running the program. Before proceeding, let's take a tour of the Main Menu and the Main Program window.

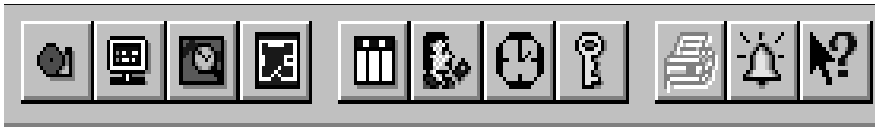


Main Program Window

The Main Program window consists of three main features: the Main Menu, the Toolbar and the Status bar.

The Main Menu allows you access to all of the features within the program. Simply click on the menu item to display its menu.

The Toolbar contains tools that allow you to move quickly to a particular screen or function. These screens and functions, as well as the tools on the Toolbar, will be described in greater detail in later chapters.



Toolbar

The Status Bar contains current information such as useful tips and the system date and time, as well as active icons. For example, you might find a communications icon which allows reconnection to the server, and an active alarm indicator which provides direct access to the Alarm Servicing window.

Using Online Help

Using Online Help is like having a user manual on your computer screen. The Help system contains specific information on all of the many screens and dialog boxes throughout the program. It not only contains general procedures and terms, but also provides context-sensitive help that displays information about the part of the NexSentry program where you currently are working.

You can access the Help option from the main menu. There are also help buttons on most of the dialog boxes that will bring up additional information about that dialog box.

To use the online Help:

1. From the Help menu, click **Index**. The help contents window appears.
2. Type the topic with which you need help. The topics will appear in the lower window as you type.
3. Double-click the topic to display the contents.

Planning the Database

Before the initial setup of the NexSentry Manager system, you must carefully consider your access control needs and formulate a plan for creating your Database. To create the Database, two specialized areas of knowledge are required:

- Hardware installation of ACUs and components controlled by NexSentry Manager.
- Site- or facility-specific knowledge of the company where the system is being installed.

Gathering Data

Before you begin entering data, gather the following information:

System Administrator Data

- Operators who will run the system and their permission levels.
- Access to the dealer/installer who installed your system (in person or via telephone).
- Appropriate installation and user's manuals.
- Copies of the NexSentry Manager Input Forms (Appendix A).
- Information about the general security needs of the facility, such as:
    - Will you have building/sector modes?
    - Will you have privileged keys?
    - What logs will be maintained?
    - What events should constitute alarms?
    - When will you transfer new information to the component parts of the system?

Hardware and Facility Data

- All information about your facility and equipment, including:
    - As-built drawings, floor plans, and/or setup sheets for monitor points and doors.
    - Quantities of all types of equipment and how connections between monitor points, doors, and ACUs have been made (usually from setup sheets).
    - Which devices have been connected with which COM ports, and the baud rates for each.

- Types of cards (1030, 1040, 1050, 1060, Magnetic Stripe, Smart Card or Digital) and facility code (1030 and 1040 cards only).

Cardholder Data

- A complete listing of all employees who will be cardholders along with whatever information about them that you want to include in your Database.
- Work schedules for employees in each department.
- Which employees normally use which doors.
- Key codes for the cards to be assigned.

Tip

You will only have to undertake this large task once if you properly back up your Database at regular intervals. Check with your installer to see if this has already been setup. See *Backing Up the System Page 5-15*

Completing the Input Forms

In Appendix A of this guide, you will find the NexSentry Manager Input Forms. The forms are the basis for the Database you will create. They serve as a guide through the data-collection process, helping you to organize information on paper, in a manner that will speed data entry into the NexSentry Manager.

Forms contain two kinds of data:

- **Cardholder data** describes who can have access, and where and when access is allowed; it includes information about cardholders and groups of cardholders, including access codes, and time periods.
- **System data** are the standing instructions for your facility's configuration of NexSentry Manager. System data describes door and sensor locations, which events will cause alarms, and other information that makes your setup unique.

Tip

You will find the Input Forms in Appendix A. You can use these as photocopy "master sheets" in order to make as many copies as you will need.

Using the Database

Navigating the NexSentry system is quick and easy. There are two ways to access information. You can choose the selection from the Main menu, or click on a tool in the Toolbar to take you quickly to the area you want. The Main menu selections and the shortcut items will be discussed later in this manual.

It is important to note the general properties of the Browse Database option. Browsing through the Database allows you to add, change, and view data for the following categories: Hardware, Personnel, System Administration, and Miscellaneous. All of the data input is made through the Browse Database option.

Browsing the Database

Browse Tool

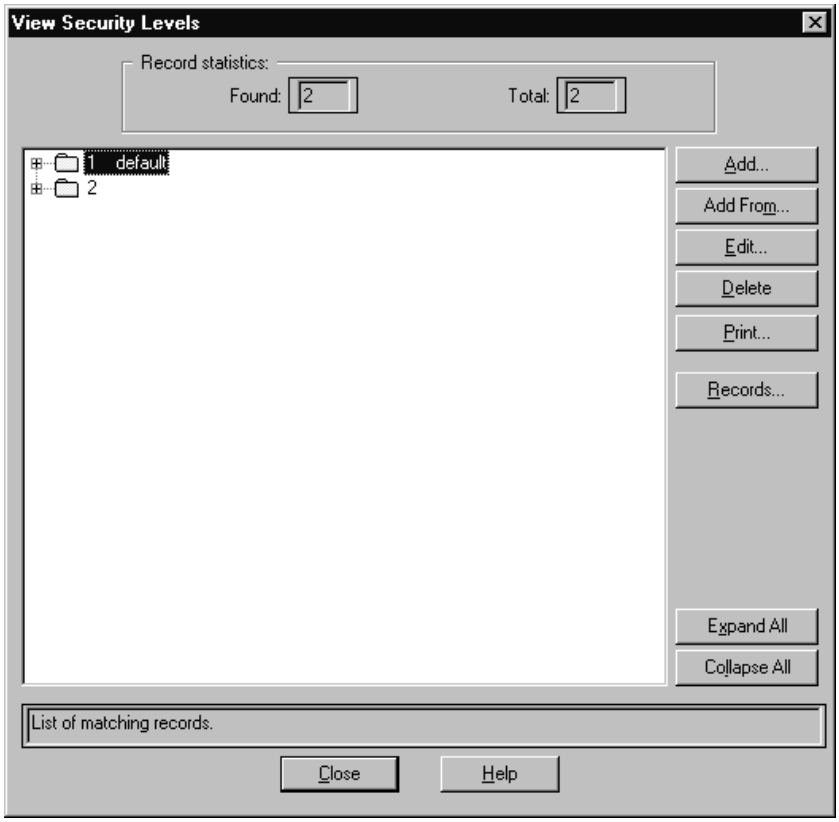
From the Database menu, click **Browse** or click on the Browse Tool in the Toolbar. This brings up the Browse Database window.

Browse Database Window

Tip

- Browsing is the easiest way to navigate through your Database. Use the Browse command or the Browse Tool when you have multiple items to view, add, or change in your Database.
- You can double-click on any of the main areas to expand to show their sub-entries, or click on **Expand All** to expand the entire list.
- Double-clicking on a sub-entry will display the View Records dialog box for that particular item. You can view or edit from the View Records dialog box.

The following functions are available when you are in a View Records dialog box: Add, Add From, Edit, Delete, Sort, Filter, Expand All, Collapse All, Refresh, and Print.



View Records Dialog Box

The following list describes the View Records dialog box buttons and functions:

Button	Description
Add	Add a new record to the Database. *Displays the add dialog box.*
Add From	Add a new record to the Database based on the values from the selected record. *Displays the add dialog box.*
Edit	Edit the selected record. *Displays the edit dialog box*.
Delete	Delete the selected records. *Displays a confirmation dialog box*.
Print	Print the selected records. *Presents the Print Setup dialog box, and then displays the report formatting dialog box to allow a report of all records in the View Records dialog box*.
Records	**Sort** - Specify sorting criteria for the records. *Brings up a dialog box that allows you to set the order in which the records* are displayed. *See* *"Sort and Filter," Page 1-16.* **Filter** - Defines a subset of the records to view *Allows you to perform basic and advanced filtering*. *See* *"Sort and Filter," Page 1-16*. **Refresh** - Updates the screen with the latest information from the Database. This will also re-access the Database if someone else is making any changes to the data.
Expand All	Expand the tree to show all items.
Collapse All	Collapse the tree to show only first-level items.

Tip

All of the dialog boxes have help text in the bottom window for the current control or field.

Sort and Filter

In addition to the View Database functions, there are other tools in the View Records dialog boxes.

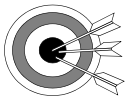
The Sort option allows you to change the order of the records that appear on the screen. This is available for all of the Database viewing options.

The Filter option allows you to control which records will appear on the active dialog box. There are two different options to the filter command:

- Basic: Quickly select the records by the ID number or Description.
- Advanced: Select records by any field or combination of fields.

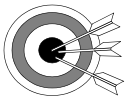
Example

To sort the record list of Cardholders by last name:



1. From the Database menu, click **Browse**.
2. Double-click **Personnel** in the Database outline to expand its sub-entries.
3. Click **Cardholders**, and then click **Edit**. You can also double-click **Cardholders**. This will display the View Records dialog box.
4. Click **Sort**. This will display the sort dialog box.
5. Click on **Last Name** in the fields column and then click **Move First**.
6. Click on **OK** to return to the View Records dialog box. The View Records dialog box returns with the record list sorted by last name. To undo the effects of sorting, select **Sort** again and click **OK**. The View Records dialog box returns with the record list in its original state.

Example



To filter just those cardholders with the last name of Smith:

1. From the Database menu, click **Browse**.
2. Double-click **Personnel** in the Database outline to expand its sub-entries.
3. Click **Cardholders**, and then click **Record**. This will display the View Records dialog box.
4. Select **Filter**. This will display the **Basic Filtering** dialog box.
5. Select **Advanced**. This will display the advanced filter dialog box.
6. Click on **Last Name** in the fields column and then type "**`Smith`**" next to text in the value field.
7. Click **Add to Query**.
8. Click **OK** to filter the records and to return to the View Records dialog box. To undo the effects of filtering, select **Filter** again, and click on **Clear**. Click **OK**, and the View Records dialog box returns with the record list in its original state.

Note

*The **Refresh** button searches the Database using the same criteria you have selected. This is needed if someone else might be working on the same set of records and making changes.*

After adding an item, any sort or filter criteria are lost. You are then presented with the complete list of all the records sorted by ID numbers.

Chapter 2
System Administration Data

Chapter Overview

This chapter covers the viewing, editing and configuring of the system administration functions.

- About System Admin Page 2-2
- Using System Admin Screens Page 2-3
- Security Levels Page 2-4
- System Users Page 2-6
- ACU Users Page 2-8
- Transactions Page 2-10
- Alarm Responses Page 2-12
- Audit Trail Page 2-13
- User Defined Fields Page 2-14
- Facility Codes Page 2-16
- Time Codes Page 2-17
- Time Groups Page 2-19
- Holidays Page 2-20
- Actions Page 2-21
- Action Groups Page 2-23
- Maps Page 2-25
- Sounds Page 2-26
- System Defaults Page 2-27

Key Terms

- **System User:** *A user is an operator with a password who is authorized to use the NexSentry Manager.*
- **Security Level:** *A defined list of permissions available in the NexSentry Manager. Assignment of a Security Level to a System User determines what the user may do.*
- **ACU User:** *A user that is authorized to access ACUs directly via the ACU Terminal port. This information is downloaded to the ACUs.*
- **ACU User Rank:** *The predefined level of permission that an ACU User may have. This rank determines what the ACU User may do with the ACU when connected directly to the ACU. See the ACU manual fora description of available Ranks.*

About System Admin

Many NexSentry Manager System Administration activities are routine procedures concerned with system change and growth, as well as regular maintenance activities, such as Database backup and archiving. Most system administration procedures, such as adding or deleting a cardholder, are simple, one-step operations. Others, such as removing monitors and relays, involve more complex changes to the Database and may even require disconnecting hardware devices.

During Installation, the system administration data should be entered before you enter hardware or cardholder information. Many of the hardware and facility devices require data from the system administration fields. You should refer to the completed data forms for the information for each of the following sections.

Tip

Always back up your Database before you prepare to make complex Database changes, remove monitors or relays, or disconnect hardware. *See "Backing Up the System," Page 5-15.*

Using System Admin Screens

You can access all of the System Administration configuration Screens from the Browse Database function.

1. From the Database menu, click **Browse** or select the Browse Database tool.
2. Double-click **System Administration** in the Database outline to expand its sub-entries.
3. Click the desired system administration activity, and then click **View** or double-click the desired item to bring up the View Records dialog box.

Browse Tool

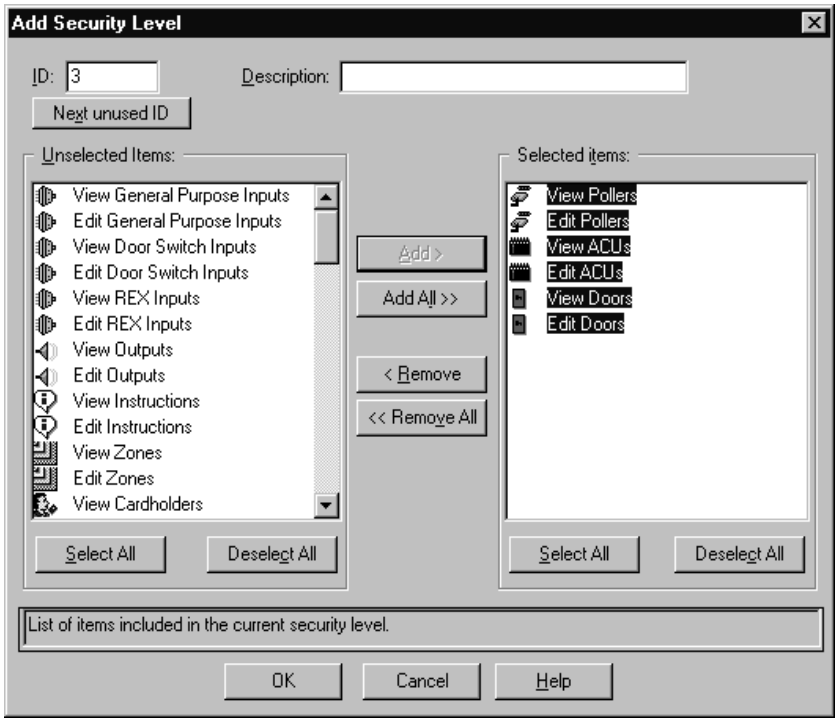
The following sections describe the System Administration functions and the unique information required.

Security Levels

Security levels determine which system users have access to different portions of the NexSentry Manager software. You can define the number of security levels and limit access to various NexSentry Manager functions based on your needs.

To view Security Levels:

1. From the Database menu, click **Browse**.
2. Double-click **System Administration** to expand its sub-entries.
3. Double-click **Security Levels**.
4. Click **Add.**

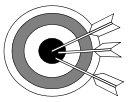


Add and Edit Security Level Dialog Box

5. The Add Security Level dialog box allows you to define an ID number, a description of the security level, and the defined items or areas that will be available to that particular security level. The defined items appear in the dialog box in the left window. You can click on individual items or select the entire list by clicking **Select All.**

6. When you have finished selecting items from the unselected item list defined items are selected you can add them to the selected points list on the right. These will be the selected areas that will be accessible for this particular security level.
7. Enter data into each field as appropriate for Security Levels by referring to the completed data forms.
8. To save your changes and exit the Add Security Levels dialog box, click **OK**. The View Security Levels dialog box returns with the entry on the record list.

Example



For instance, if you were going to set up a new security level that had the right to view cardholder information, but not to edit it, you would select **View Cardholders** from the list on the left and click **Add** to place this in the list to the right, then click **OK** to save.

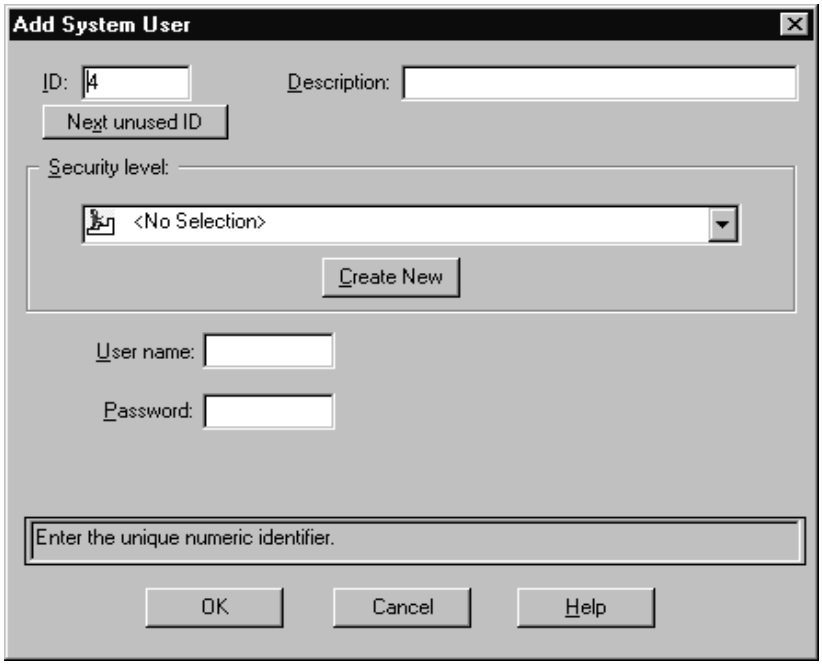
System Users

A system user is an operator with a password who has permission to log into the Client. A user may be able to change or add Database information, add cardholders, lock and unlock doors, or back up the Database depending on the Security Level you have previously set.

In the Add System User dialog box, you can assign the ID number, a description, the security level, the user name and password for the new user.

To view System Users:

1. From the Database menu, click **Browse**.
2. Double-click **System Administration** to expand its sub-entries.
3. Double-click **System Users**.
4. Click **Add.**



Add and Edit System User Dialog Box

5. Enter data into each field as appropriate for System Users by referring to your completed data forms.

6. To save your changes and exit the Add System Users dialog box, click **OK**. The view System Users dialog box returns with your entry on the record list.

Tip

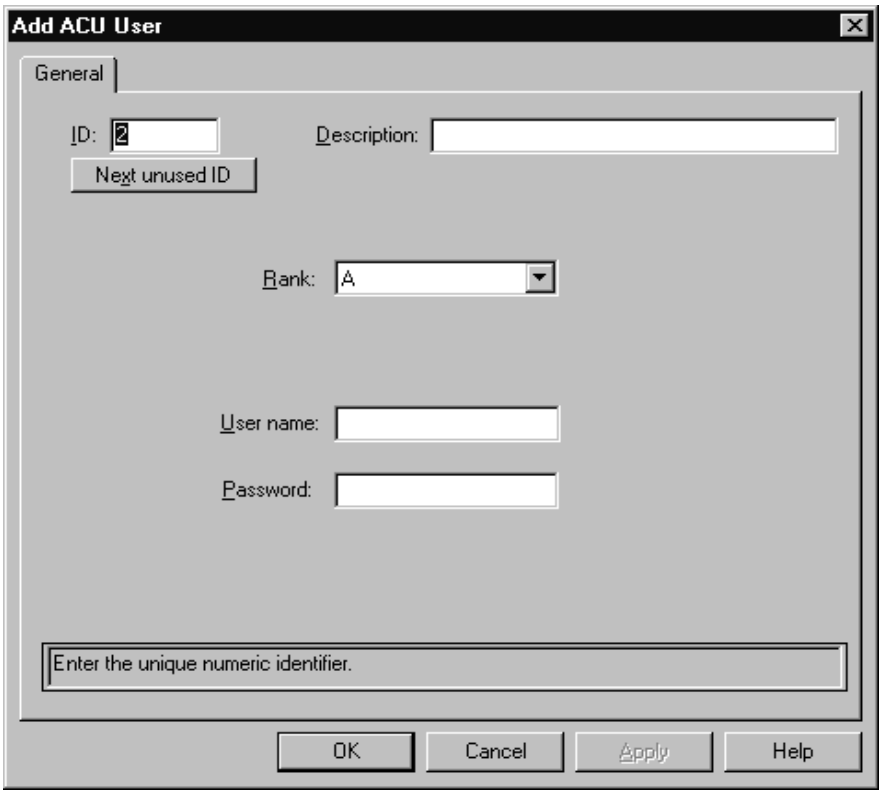
The Password will not be displayed when you type it. Only asterisks will appear for each character you type. The dialog box will prompt you to retype the password to confirm that you have entered it correctly.

ACU Users

An ACU user is an operator with a password who has the ability to control individual components of the system directly from the ACU. NexSentry Manager does not allow more than eight operator passwords.

To view ACU Users:

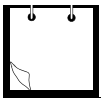
1. From the Database menu, click **Browse**.
2. Double-click **System Administration** to expand its sub-entries.
3. Double-click **ACU Users**.
4. Click **Add.**



Add and Edit ACU Users Dialog Box

5. Enter data into each field as appropriate for the ACU users by referring to the completed data forms.
6. To save your changes and exit the Add ACU Users dialog box, click **OK**. The view ACU Users dialog box returns with the entry on the record list.

Note



In the view/edit ACU User dialog box you can assign the rank (A-F) for the ACU user. See the ACU manual for description of available ranks.

When communicating directly with an ACU through a terminal program, only the password is used. The default password for all of the ACUs is **new***. The System Administrator should change this password after the installation is complete or when configuring ACU Users. Also see* *"Addressing ACUs," Page 3-5**.*

Transactions

Transactions define the manner in which system activities are displayed and stored. There are two folders in System Administration that concern Transactions: Transaction Log and Transaction Types. The Transaction Log stores all of the transactions from all of the ACUs on the system. This includes all of the transactions from the Monitor window and those transactions pushed off the Monitor window. The Transaction Log features are described in "Monitoring Current Transactions," Page 5-2.

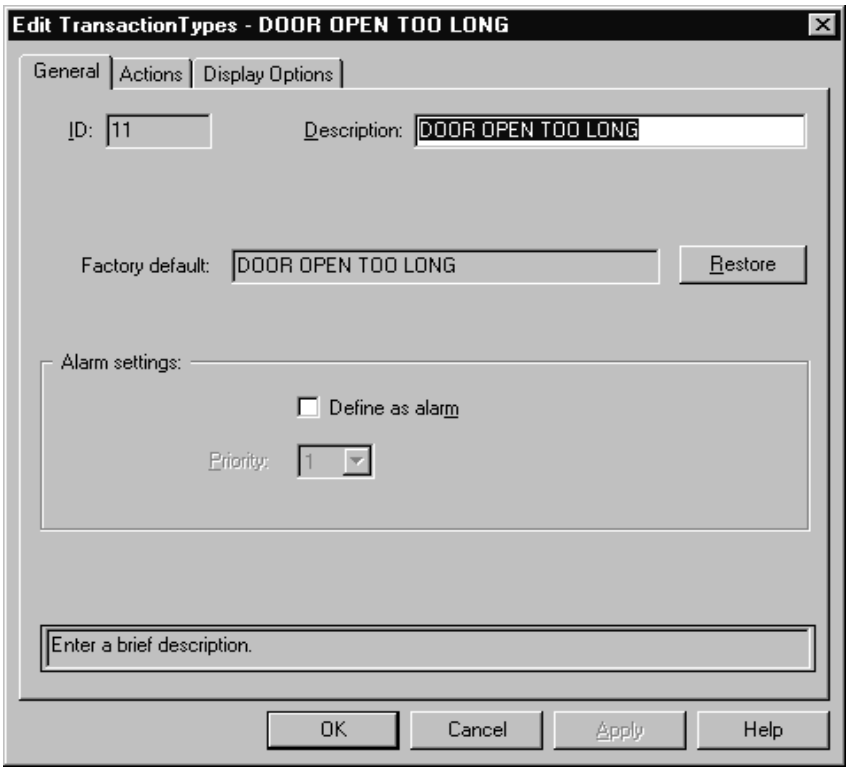
The Transaction Types folder allows you to configure the way in which the Transactions are displayed on the system. In the Edit Transactions Type dialog box, you can view or edit the transaction type, configure the color, the sound, and even designate a specific transaction as an alarm.

To view Transaction Log:

1. From the Database menu, click **Browse**.
2. Double-click **System Administration** to expand its sub-entries.
3. Double-click **Transactions** to expand its sub-entries.
4. Double-click **Types**.
5. Click on the transaction you want to modify and click **Edit.**

There are three pages to the Add and Edit Transaction Types dialog box:

- General
- Actions
- Display Options



Add and Edit Transaction Types Dialog Box

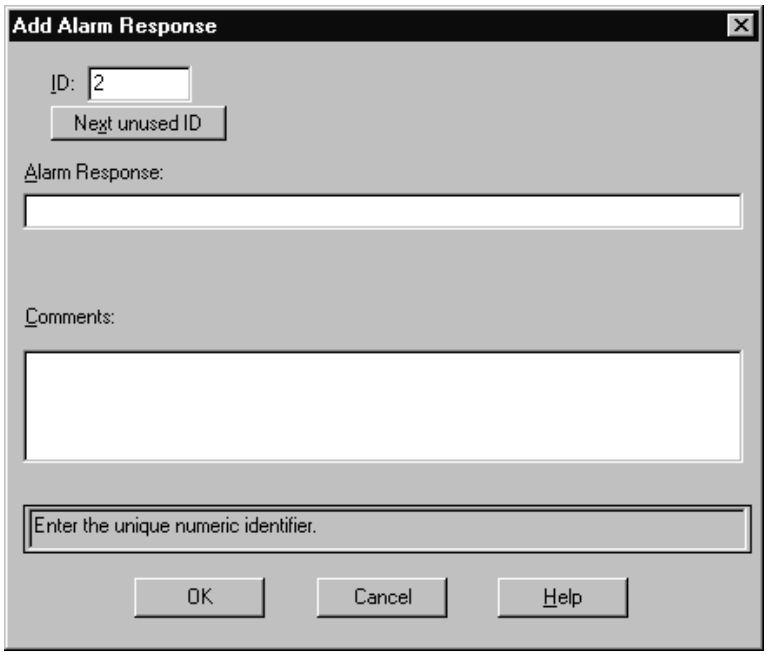
6. Enter data into each field as appropriate for Transactions Log by referring to the completed data forms.
7. To save your changes and exit the Add Transactions Log dialog box, click **OK**. The view Transactions Log dialog box returns with your entry on the record list.

Alarm Responses

You can define an Alarm Response for any given alarm. In the Add Alarm Response dialog box, you can choose the unique ID number, a description of the Alarm Response and additional text or comments about the Alarm Response.

To view Alarm Responses:

1. From the Database menu, click **Browse**.
2. Double-click **System Administration** to expand its sub-entries.
3. Double-click **Alarm Responses**.
4. Click **Add.**



Add and Edit Alarm Response Dialog Box

5. Enter data into each field as appropriate for Alarm Responses by referring to the completed data forms.
6. To save your changes and exit the Add Alarm Responses dialog box, click **OK**. The view Alarm Responses dialog box returns with your entry on the record list.

Audit Trail

The Audit Trail is a system administrator tool for tracking all of the changes made to the database. The Audit Trail adds a record every time a system user adds, edits, or deletes system information.

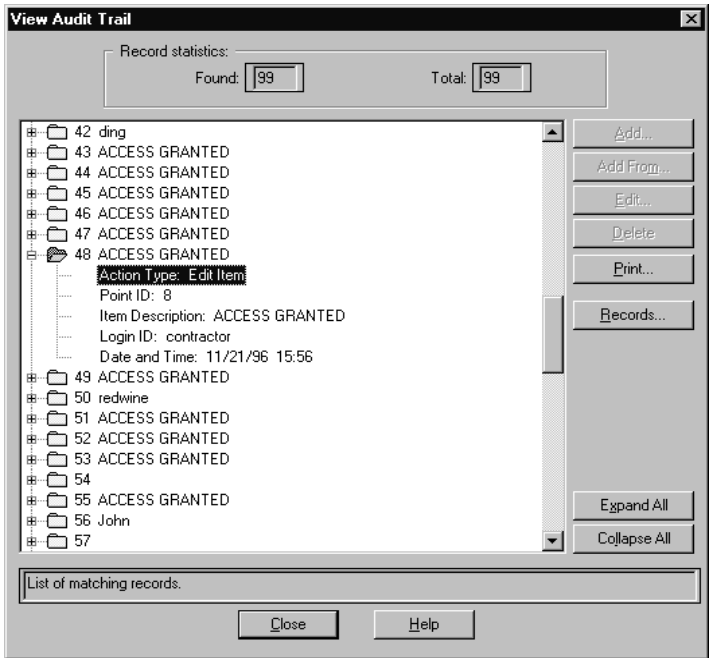
Audit Trail records the following information:

- Activity Type: Add, Edit or Delete.
- Point ID: The ID number of the item modified.
- Item Description: The description of the item modified.
- Login ID: The Login ID of the system user making changes.
- Date and Time: The date and time of the changes.

To view the Audit Trail:

1. From the Database menu, click **Browse**.
2. Double-click **System Administration** to expand its sub-entries.
3. Double-click **Audit Trail**.

There is only the **View** dialog box for the Audit Trail. You can't **Add, Add From, Edit** or **Delete** records in this dialog box.



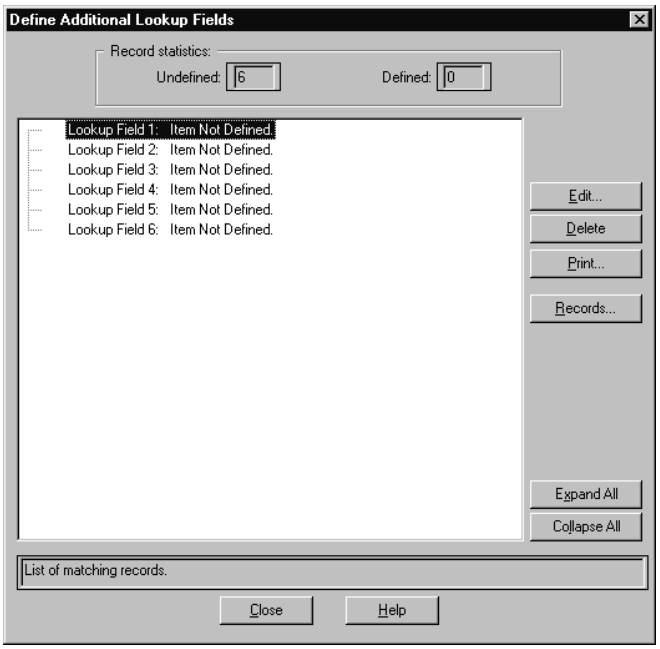
View Audit Trail Dialog Box

User Defined Fields

User-defined fields allow you to create labels and data tables for information on the cardholder dialog box. This allows you to tailor Cardholder data in a way that best suits your needs. These fields may be used for Filtering and Sorting Cardholder records.

To view User Defined Fields:

1. From the Database menu, click **Browse**.
2. Double-click **System Administration** to expand its sub-entries.
3. Double-click **User Defined Fields** to expand its sub-entries.
4. Double-click **Additional Text Fields** or **Additional Lookup Fields.**



Add and Edit User Defined Fields Dialog Box

5. Click the field that you want to modify and click **Edit.**

Note

You can't add any more records to the Additional Lookup Fields or the Additional Text Fields. You can only edit the existing records. If the record has not been changed, it will indicate "Item Not Defined."

6. Enter data into each field as appropriate for Additional Text or Lookup fields by referring to the completed data forms.

7. To save your changes and exit the Edit Text Fields or Additional Lookup dialog boxes, click **OK**. The view records dialog box returns with your entry on the record list.

Tip

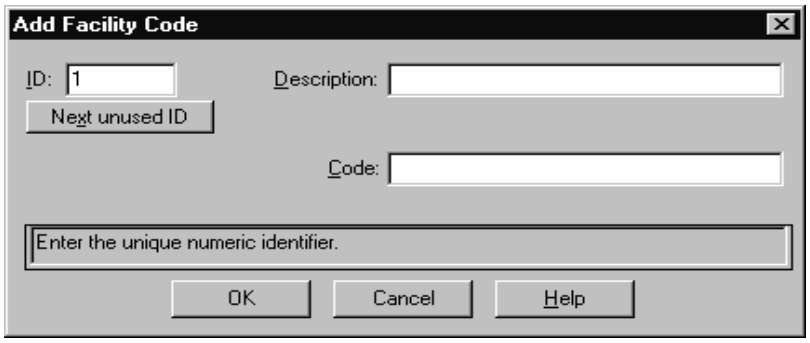
You will need to define the User Defined Fields that you plan on using before you enter any Cardholder Information.

Facility Codes

Facility codes are the unique identification number assigned to a facility, which allows additional access control. Facility codes are available only for 1030 and 1040 key cards.

To view Facility Codes:

1. From the Database menu, click **Browse**.
2. Double-click **System Administration** to expand its sub-entries.
3. Double-click **Facility Codes**.
4. Click **Add.**



Add and Edit Facility Codes Dialog Box

5. Enter data into each field as appropriate for Facility Codes by referring to the completed data forms.
6. To save your changes and exit the Add Facility Codes dialog box, click **OK**. The view Facility Codes dialog box returns with your entry on the record list.

Miscellaneous

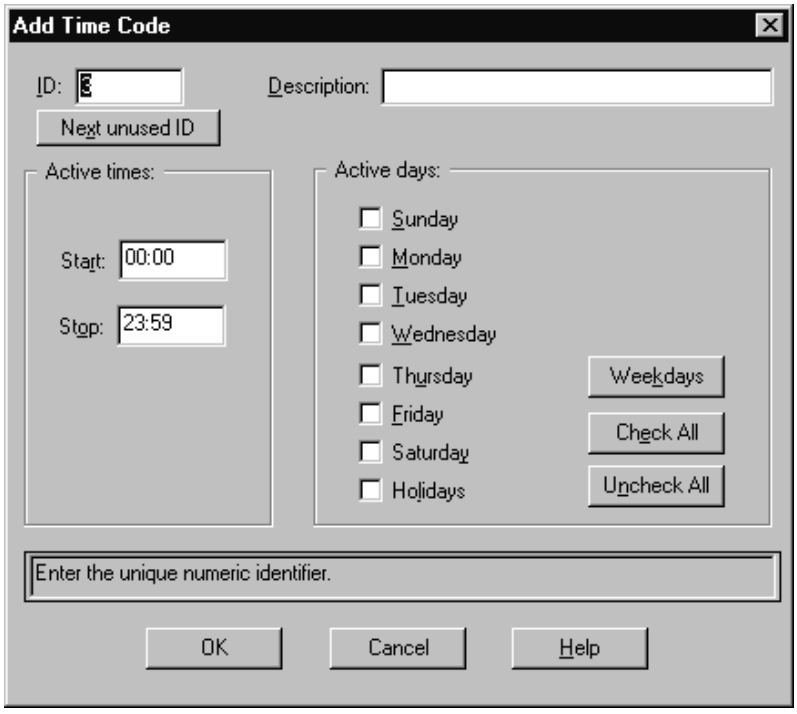
The Miscellaneous screens are really more System Administration screens. This area contains the dialog boxes for setting the Time Codes and Time Groups, Holidays, Action Codes and Action Groups, Maps, and the System Sounds. These are basic system features that should be configured along with all of the other System Administration functions.

Time Codes

A Time Code is a definition of the time of day and days of the week when events are to occur. They are used in assigning access privileges, performing scheduled tasks, and monitoring access points.

To view Time Codes:

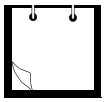
1. From the Database menu, click **Browse**.
2. Double-click **Miscellaneous** to expand its sub-entries.
3. Double-click **Time Codes**.
4. Click **Add.**



Add and Edit Time Codes Dialog Box

5. Enter data into each field as appropriate for Time Codes by referring to the completed data forms. To save your changes and exit the Add Time Codes dialog box, click OK. The view Time Codes dialog box returns with your entry on the record list.

Note



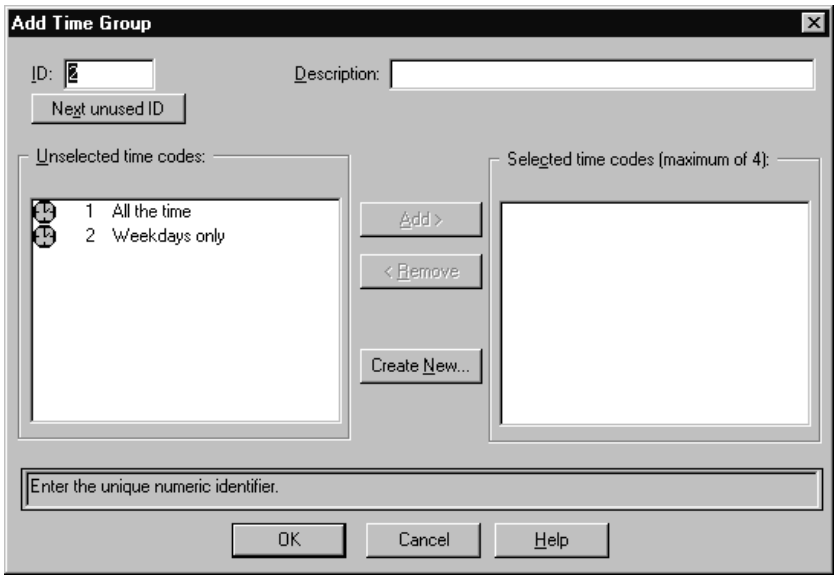
There can only be 4 time periods in a Time Group!

Time Groups

Time Groups are simply the grouping of time codes. For instance, you could create a group that used the swing shift time code and also included Saturday morning.

To view Time Groups:

1. From the Database menu, click **Browse**.
2. Double-click **Miscellaneous** to expand its sub-entries.
3. Double-click **Time Groups**.
4. Click **Add.**



Add and Edit Time Groups Dialog Box

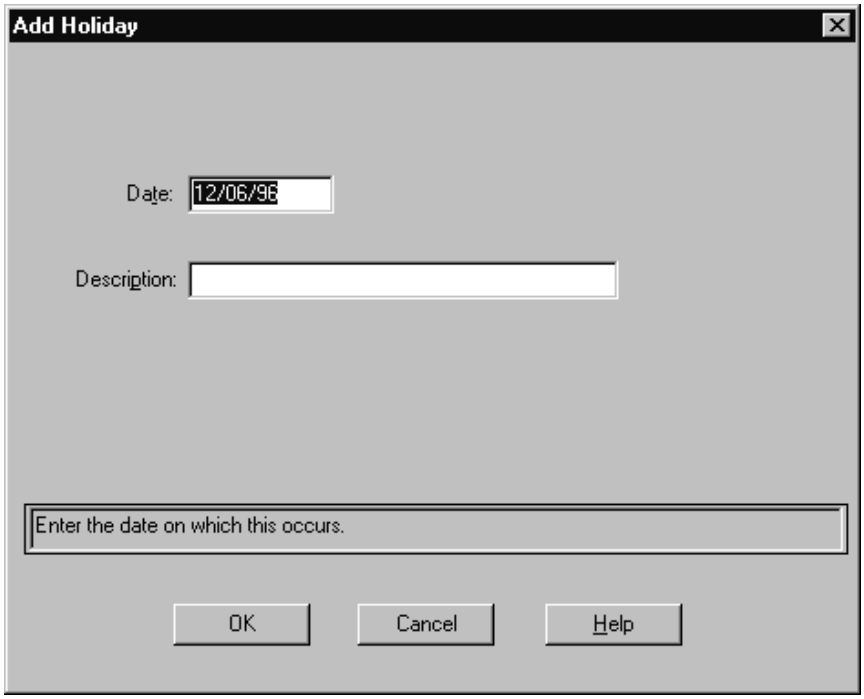
5. Enter data into each field as appropriate for Time Groups by referring to the completed data forms.
6. In the left window, select the Time Codes that will be included in this Time Group and click **Add**.
7. To save your changes and exit the Add Time Groups dialog box, click **OK**. The View Time Groups dialog box returns with your entry on the record list.

Holidays

The Holidays dialog box is used to set the specific dates for holidays.

To view Holidays:

1. From the Database menu, click **Browse**.
2. Double-click **Miscellaneous** to expand its sub-entries.
3. Double-click **Holidays.**
4. Click **Add.**



Add and Edit Holidays Dialog Box

5. Enter data into each field as appropriate for Holidays by referring to the completed data forms.
6. To save your changes and exit the Add Holidays dialog box, click **OK**. The view Holidays dialog box returns with your entry on the record list.

Actions

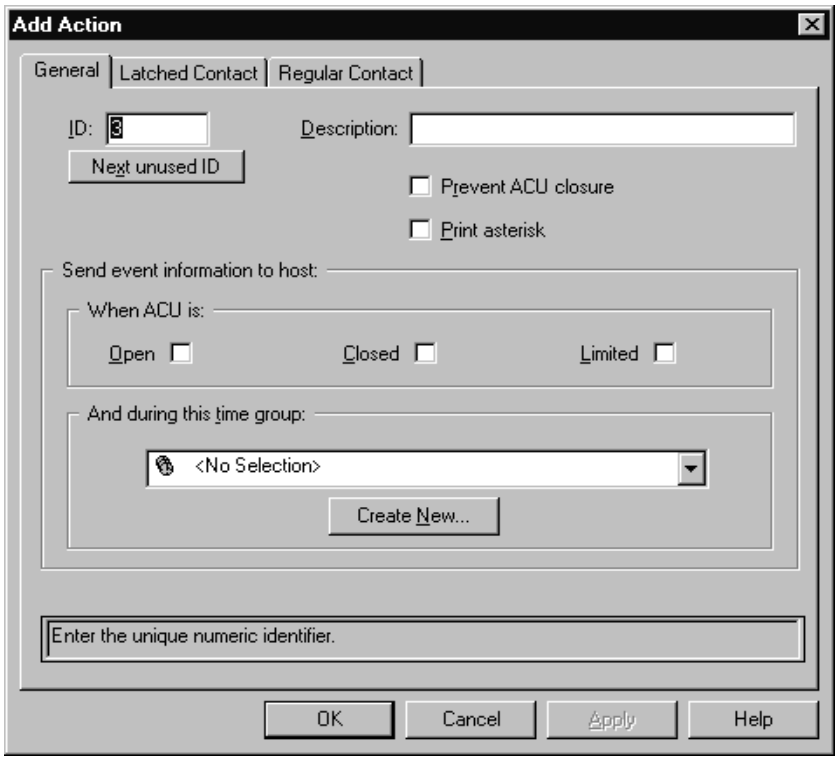
Actions define how individual ACUs react to events occurring within them. Configuration of ACU actions does not affect how the NexSentry Manager software reacts to the events. Once an action has been created and assigned, it is downloaded to each appropriate ACU to control how that ACU will react when that event occurs.

To view Actions:

1. From the Database menu, click **Browse**.
2. Double-click **Miscellaneous** to expand its sub-entries.
3. Double-click **Actions**.
4. Click **Add.**

There are three pages to the Add and Edit Actions dialog box:

- General
- Latched Contact
- Regular Contact



Add and Edit Actions Dialog Box

5. Enter data into each field as appropriate for Actions by referring to the completed data forms.
6. To save your changes and exit the Add Actions dialog box, click **OK**. The view Actions dialog box returns with your entry on the record list.

Action Groups

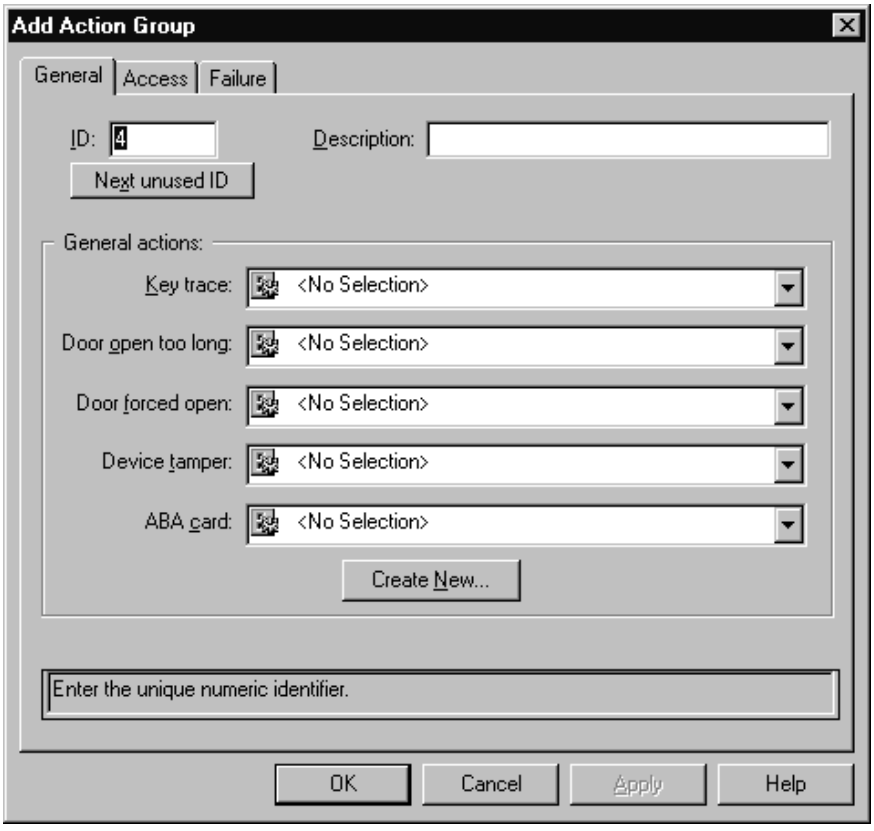
Action Groups are the grouping of individual Action codes for use with perimeter Doors. For instance, you could group together all of the common Action codes in one Action Group.

To view Action Group:

1. From the Database menu, click **Browse**.
2. Double-click **Miscellaneous** to expand its sub-entries.
3. Double-click **Action Group.**
4. Click **Add.**

There are three pages to the Add and Edit Action Group dialog box:

- General
- Access
- Failure



Add and Edit Action Group Dialog Box

5. Enter data into each field as appropriate for Actions by referring to the completed data forms.
6. Select the Actions that will be grouped together from the pull-down entry fields.
7. To save your changes and exit the Add Actions dialog box, click **OK**. The view Actions dialog box returns with your entry on the record list.

Maps

The Maps folder in the Browse Database window does not allow you to view or modify the maps. The purpose is to allow you to view a list of the defined maps and which icons are included in each map.

Map Tool

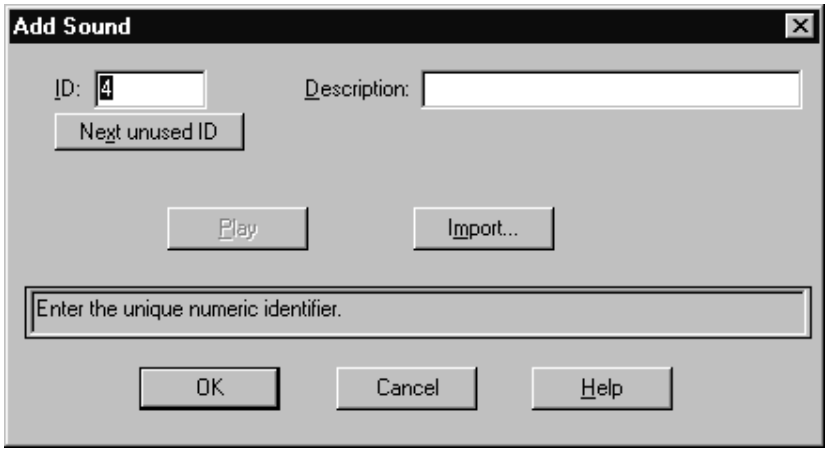
To create, modify and view system Maps, you must use the Map Tool Icon from the Toolbar or select Maps from View in the Main Menu. *For more detail see "Maps," Page 3-17.*

Sounds

The Sounds dialog box is used to set the specific sound files that will be used for alarms. If your system has a sound card you can use WAV files that will produce the audio portion of the Alarm.

To view Sounds:

1. From the Database menu, click **Browse**.
2. Double-click **Miscellaneous** to expand its sub-entries.
3. Double-click **Sounds**.
4. Click **Add.**



Add and Edit Sounds Dialog Box

5. Enter data into each field as appropriate for your Sounds settings.
6. Click the Import button to select the file you want for that sound definition. This will bring up the select files dialog box that will allow you to select a WAV file.
7. To save your changes and exit the Add Sounds dialog box, click **OK**. The view Sounds dialog box returns with your entry on the record list.

Tip

You must first add the sounds to the NexSentry Manager in the above steps before you can use them in Alarms. Once the sound is defined, you can designate particular transactions as alarms. See "Transactions," Page 2-10.

To use the sound features, you must also have your Sound Card configured for your computer through the Control Panel.

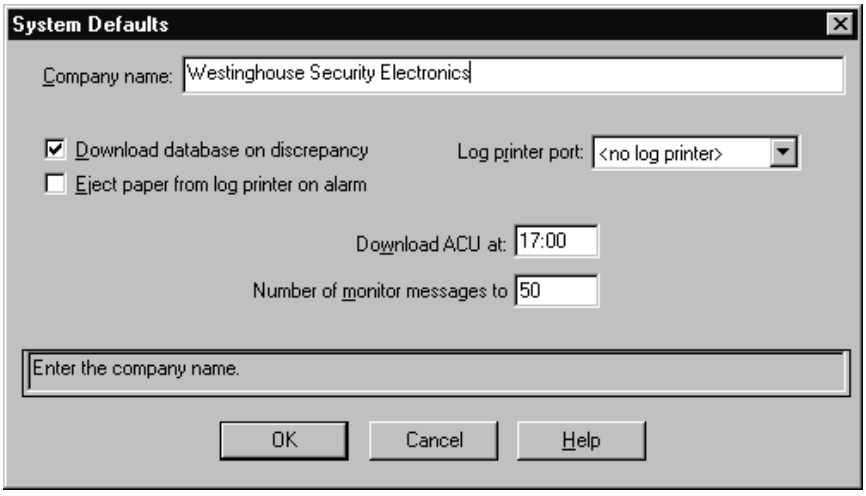
System Defaults

The System Defaults dialog box allows you to specify the following default system settings:

- Company name—Specifies the heading to be used for Reports.
- Download Database on discrepancy—Downloads Database to all ACUs if differences are found between information in the ACU and the information stored in the Database.
- Eject paper from log printer on alarm—Causes a form feed at the log printer when a transaction defined as an alarm occurs.
- Download ACU at—Specifies the time and/or date when the ACUs are downloaded if the Download on discrepancy is not set.
- Number of Monitor messages to—Defines the number of messages that will appear on the Monitor at any one time.

Accessing the System Defaults Dialog box

1. From the Database menu, click **System Defaults**.
2. Change the system defaults as needed.
3. Click **OK** to save changes.



System Defaults Dialog Box

Tip

Choose a time that has less activity on the system to download to the ACUs.

The more Monitor messages you have displayed, the slower the program will run. Choose a number that will let you adequately monitor the system without slowing it down too much.

Chapter 3
Hardware and Facility Data

Chapter Overview

Entering the hardware and facility data is a process by which you tell the NexSentry Manager which devices you have installed within the system. This chapter covers the steps in which you enter the information.

- Using Hardware Screens Page 3-2
- Pollers Page 3-3
- Access Control Units (ACU) Page 3-5
- Doors Page 3-9
- Inputs Page 3-11
- Outputs Page 3-13
- Instructions Page 3-15
- Zones Page 3-16
- Maps Page 3-17

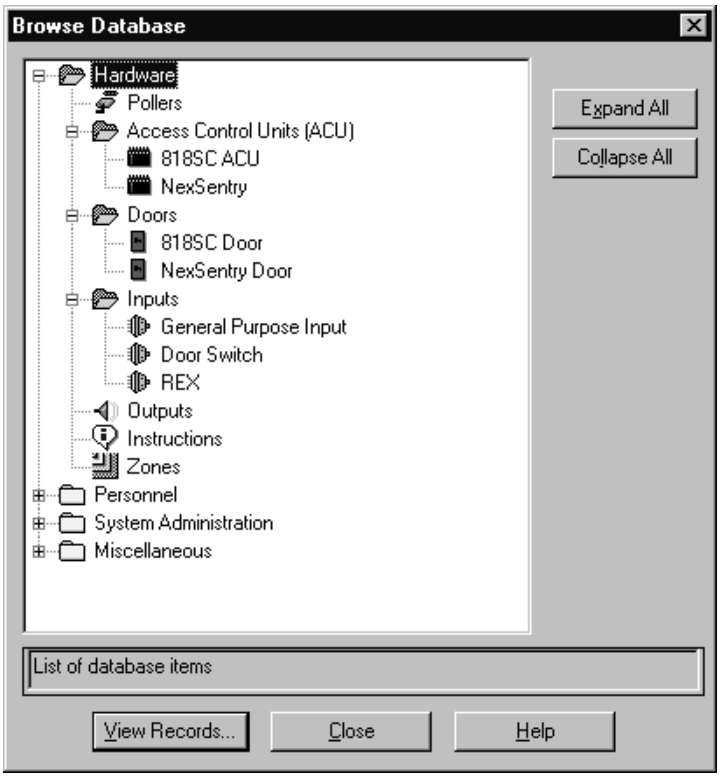
Key Terms

- **ACU:** *Access Control Unit. ACUs are the "brains" of the access control system. They control individual doors, grant access and monitor other devices and report this information to the NexSentry Manager. There are two types of ACUs used with NexSentry Manager: 818SC and NexSentry Controller.*
- **REX:** *Request for Exit, usually a switch used to leave an area through a secured door.*
- **Anti-Passback:** *A control measure that prevents a Cardholder from reusing a door prior to using an exit through another door. The term comes from an unsecure practice of employees "passing back" their cards to another employee.*
- **Auto-Forgive:** *Resets the ACUs when the Anti-Passback measure is enabled. It makes the ACUs "forget" the Anti-Passback status until a Cardholder enters through another door.*

Using Hardware Screens

You can access all of the Hardware Screens from the Browse Database function. From the Database menu, click **Browse** or click on the Browse Tool in the toolbar. This will bring up the Browse Database dialog box.

Browse Tool



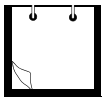
Browse Database Window

Tip

*To edit a particular piece of hardware, highlight the item and click **Edit** or just double-click the item to bring up the view dialog box for that device.*

The following sections are a description of the hardware devices and the necessary items to properly configure them.

Note



All of the Hardware devices installed in this chapter are numbered consecutively in the ID number field. For example, if you install your first Poller, it will be numbered "1." The second device you install will be numbered "2." The NexSentry Manager does this in order to uniquely identify each piece of hardware installed in the system. .

Pollers

A Poller is a NexSentry Manager element that controls communications with devices in the access control system. A Poller can communicate through only one serial port at a time, but can talk to all of the access control devices connected to that serial port at the same time. Pollers must be assigned to a particular communications port on the computer, but can be reassigned to a new port if required.

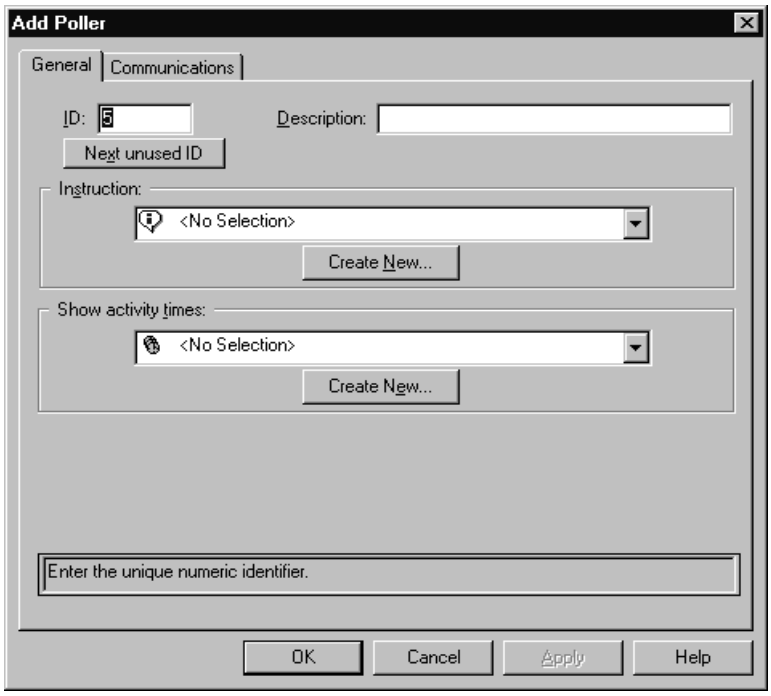
Entering Data

To view Pollers:

1. From the Database menu, click **Browse**.
2. Double-click **Hardware** to expand its sub-entries.
3. Double-click **Pollers**.
4. Click **Add**.

There are two pages to the Poller Edit dialog box:

- General
- Communications



Poller Add and Edit Dialog Box

5. Enter data into each field as appropriate for the access control system by referring to the completed data forms.
6. To save your changes and exit the Add Poller dialog box, click **OK**. The view Poller dialog box returns with your entry on the record list.

Tip

*You can add other pollers by clicking **Add**, which will present an empty Add Poller dialog box or by selecting an existing Poller record and clicking **Add From**. This will present the Add Poller dialog box with the data from the selected record already entered. You will, of course, need to enter the new ID number and Description and any other unique data to this new Poller.*

*The **Add From** option works on most of the Add and Edit dialog boxes.*

7. When you are finished, Click **OK** to close the view window and return to the Browse Database dialog box.

Access Control Units (ACU)

The Access Control Unit (ACU) is the "brains" of the access control system. ACUs control door access, and report all status of the devices related to that door (such as door monitors and card readers) to the NexSentry Manager. The NexSentry Manager downloads all of the information that the ACU requires to control its doors and devices. There are two types of ACUs used with NexSentry Manager: 818SC and NexSentry Controller.

Addressing ACUs

To configure ACUs so they can communicate with NexSentry Manager, you must first use a terminal emulation program, such as Hyperterminal in the Windows NT Accessories program group. Hyperterminal allows the computer to serve as an input/output terminal to communicate with the ACU. Using a COM port, you can communicate with one ACU at a time via its terminal port.

You must first "Address" the ACUs so that the NexSentry Manager will be able to locate them.

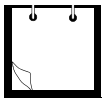
Information needed to address an ACU:

- The ACU address. This will be the same address that you will use when configuring the system later in this section. Refer to your ACU NexSentry Manager Input Form.
- Baud Rate for the ACU. The ACU may be at its default rate of 300 if the Installer has not changed it. Consult the installer for the proper baud rate.
- The COM settings. Configure Hyperterminal to use the communications settings of 7 Data bits, Odd Parity, and 1 Stop Bit (7-O-1). Some ACUs may use other settings, so refer to the installer.

Baud Rate Tips

- 9600 baud is the default baud rate for NexSentry Manager.
- Each ACU that uses the same COM port must use the same baud rate.
- Direct line modems must also have the same baud rate as all other ACUs on that COM port. Use the highest baud rate available.

Note



The default baud rate for the ACU is 300. This should not be confused for the NexSentry Manager default baud rate. The reason the ACU baud rate is so slow is that some older installations had simple communications devices that were only capable of 300 baud. You should use the 9600 baud rate for all of the ACUs in order to maximize system communication speed.

Once you have configured the COM settings Hyperterminal, perform the following to address and configure ACUs:

1. Select **Connect** to communicate with the ACU and then press the space bar. The ACU will respond: **"Password?"**
2. Type the Default password**: `NEW`** and press **Enter**.
3. You will be logged in and receive another prompt: "**Your command?"**
4. Type **`SYS`** and press **Enter.**
5. Now press Enter several times until you reach the prompt: **"Address."**
6. Enter the ACU Address number. This will be a number from 1 to 16 that you will also enter when configuring the ACU in the NexSentry Manager. Refer to the Input Form for the proper address.
7. If the ACU is running at a baud rate of less than **`9600`**, you can change that setting now as well. Type SYS and press Enter several times until you read **Host Baud.** Type **`9600`** and press **Enter**. Type **`9600`** into **Terminal Baud** and press **Enter** again**.**
8. When you are finished Addressing the ACU, press the **Escape** key, type **`Reset`** and press **Enter**. This will save the changes you have made and reset the ACU to be able to connect with NexSentry Manager. If you have changed the baud rate, reset will immediately change the baud rate to the one you set. If you still have to communicate directly, you will have to reconfigure your terminal program to use the new baud rate setting.

Tip

If you have made a mistake Addressing an ACU, return to it and do the previous steps, making corrections as necessary.

Entering ACU Data

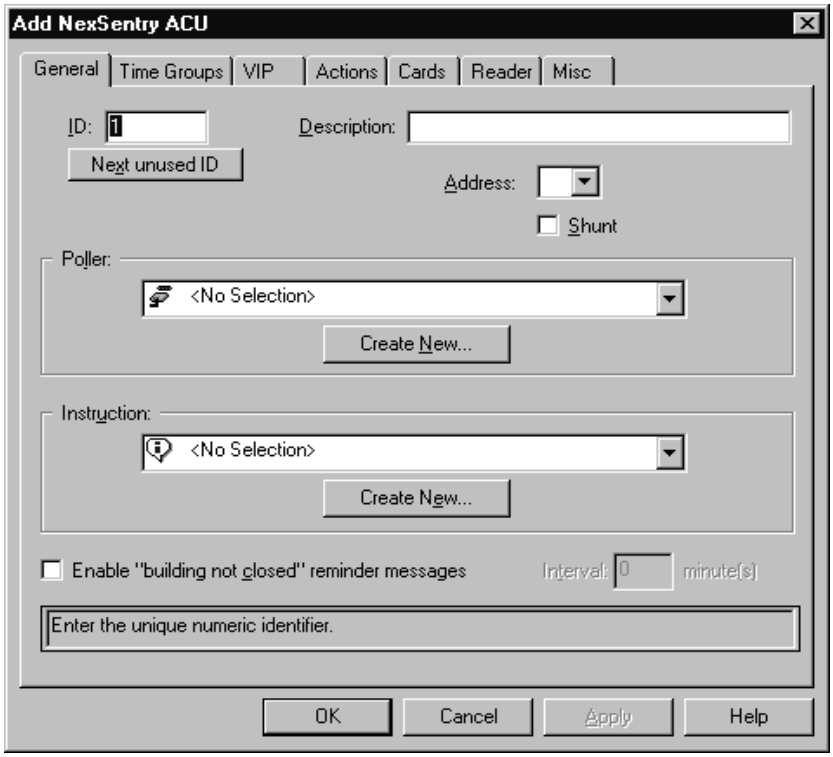
To Add ACUs:

1. From the Database menu, click **Browse**.
2. Double-click **Hardware**, then **Access Control Units** (ACU) in the Database outline to expand their sub-entries.

Click the ACU type you want, and then click **Add**. There are 7 pages to the add and edit ACU dialog box as follows:

- General
- Time Groups
- VIP
- Actions
- Cards
- Reader
- Misc

.



Add and Edit ACU Dialog Box

3. Enter data into each field as appropriate by referring to the completed data forms.

4. To save your changes and exit the Add ACU dialog box, click **OK**. This will return you to the View ACU dialog box. You will see that the ACU you have just added is now in the list.

Tip

*You can add other ACUs at this time simply by selecting **Add From** in the View window. This will allow you to create a new ACU using the settings that you used for the selected ACU.*

5. When you are finished, click **OK** to close the view window and return to the Browse Database dialog box.

Doors

In NexSentry Manager, “door” is a generic term for openings controlled by an access device, including doors, turnstiles, gates, and others. A door is always considered in relationship to the ACU to which it is connected. Different types of ACUs require different information about the doors connected to them, based on the performance capabilities of the ACU. The NexSentry Manager system knows what information each ACU requires for each door.

Information needed to address a Door

The list below includes all possible information that can be entered for doors; whether or not you will need or use all of the information depends on your system setup and the ACUs you have installed.

- Door number
- Door Description (Name)
- ACU
- ACU Sensor number
- Auto-Unlock Time Group
- Activity Time Group
- Lock Contact Point (Door Switch) and usage
- Reader type and usage
- VIP Activity
- REX Contact Point and Activity
- Anti-Passback Implementation

Entering Door Data

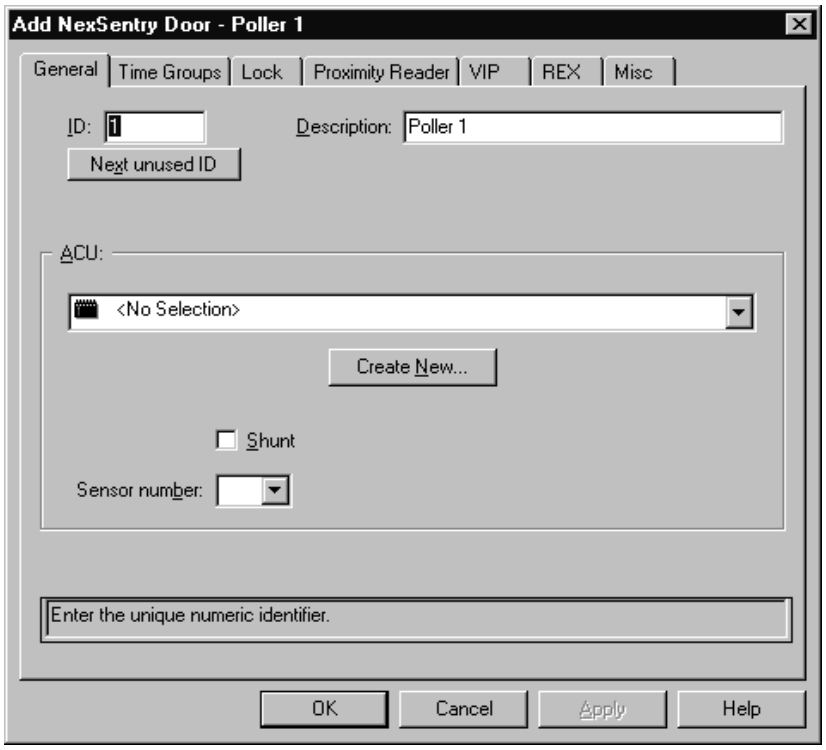
To view Doors:

1. From the Database menu, click **Browse**.
2. Double-click **Hardware**.
3. Click **Doors** in the Database outline to bring up the Add Doors dialog box and to expand their sub-entries.

The Doors Add and Edit dialog box is divided into 7 pages:

- General

- Time Groups
- Lock
- Proximity Reader
- VIP
- REX
- Miscellaneous



Add and Edit Door Dialog Box

Tip

Proximity Reader, VIP and REX are optional depending on specifics of your installation.

4. Enter data into each field as appropriate for each door by referring to the completed data forms.
5. To save your changes and exit the Add Door dialog box, click **OK**. This will return you to the View Door dialog box. You will see that the Door you have just added is now in the list.

Inputs

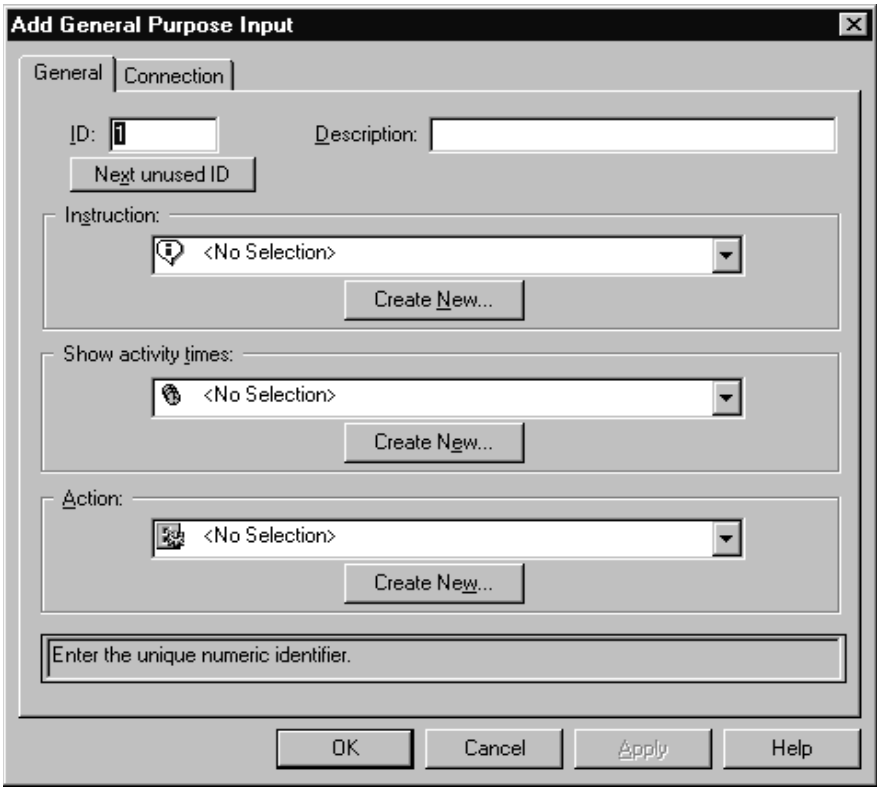
Inputs are detectors (motions sensors or temperature sensors, for example). Detectors look for changes in condition, such as an opened door contact or an activated alarm.

To view Inputs:

1. From the Database menu, click **Browse**.
2. Double-click **Hardware** to expand its sub-entries.
3. Double-click **Inputs**.
4. Click **Add**.

There are two pages to the Input Edit dialog box:

- General
- Communications



Add and Edit Input Dialog Box

5. Enter data into each field as appropriate for Input by referring to the completed data forms.

6. To save your changes and exit the Add Input dialog box, click **OK**. The view Input dialog box returns with your entry on the record list.

Tip

Inputs can be several different types, such as a General Purpose Input, a Door Switch, or a Request for Exit (REX).

Outputs

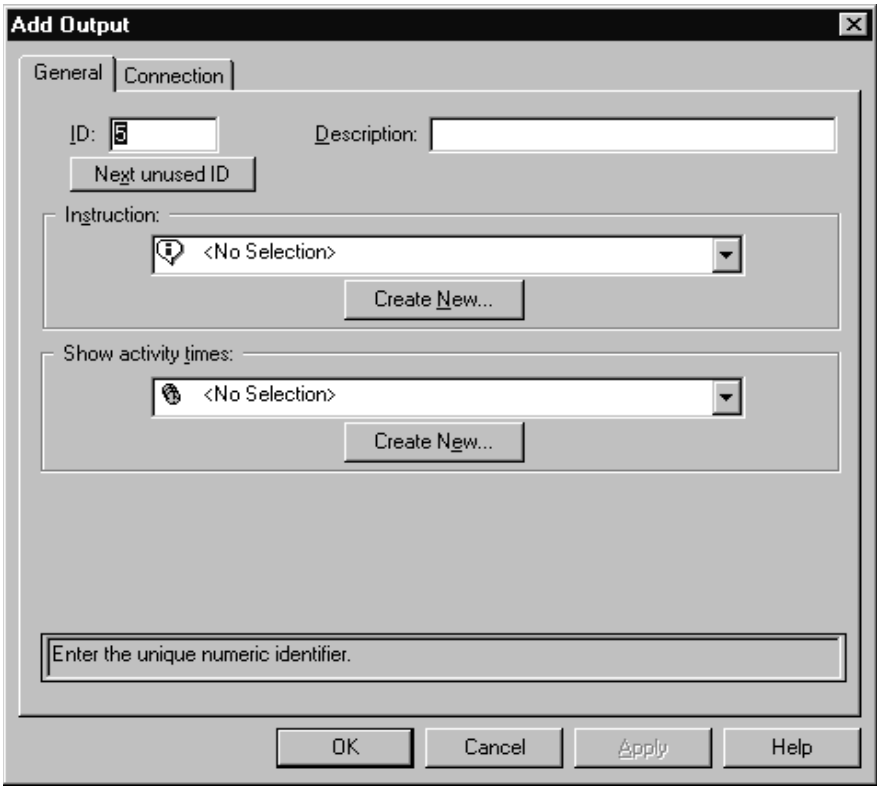
Outputs are either control or alarm devices. Control devices can be electronic door locks, lighting controllers, video monitor switches, or switches particular to the needs of an access control system. Alarm devices can be audible alarms, screen displays, or remote alarms. Alarms alert system operators or others (such as police or fire departments) to abnormal conditions.

To view Outputs:

1. From the Database menu, click **Browse**.
2. Double-click **Hardware** to expand its sub-entries.
3. Double-click **Outputs**.
4. Click **Add**.

   There are two pages to the Add and Edit Outputs dialog box:

   - General
   - Communications



Add and Edit Outputs Dialog Box

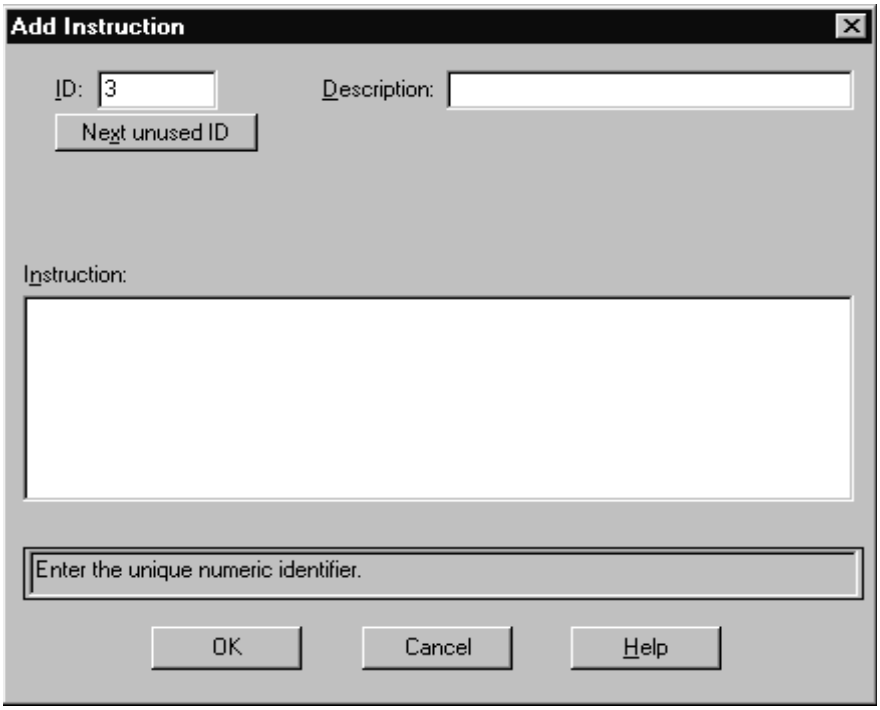
5. Enter data into each field as appropriate for Outputs by referring to the completed data forms.
6. To save your changes and exit the Add Outputs dialog box, click **OK**. The view Outputs dialog box returns with your entry on the record list.

Instructions

An instruction is a specific piece of information given to an operator when an event that requires a response occurs. Operator instructions can be tied to all individual monitor points and to log events. The NexSentry Manager system can save up to 500 separate instructions.

To view Instructions:

1. From the Database menu, click **Browse**.
2. Double-click **Hardware** to expand its sub-entries.
3. Double-click **Instructions**.
4. Click **Add.**



Add and Edit Instructions Dialog Box

5. Enter data into each field as appropriate for Instructions by referring to the completed data forms.

6. To save your changes and exit the Add Instructions dialog box, click **OK**. The view Instructions dialog box returns with your entry on the record list.

Zones

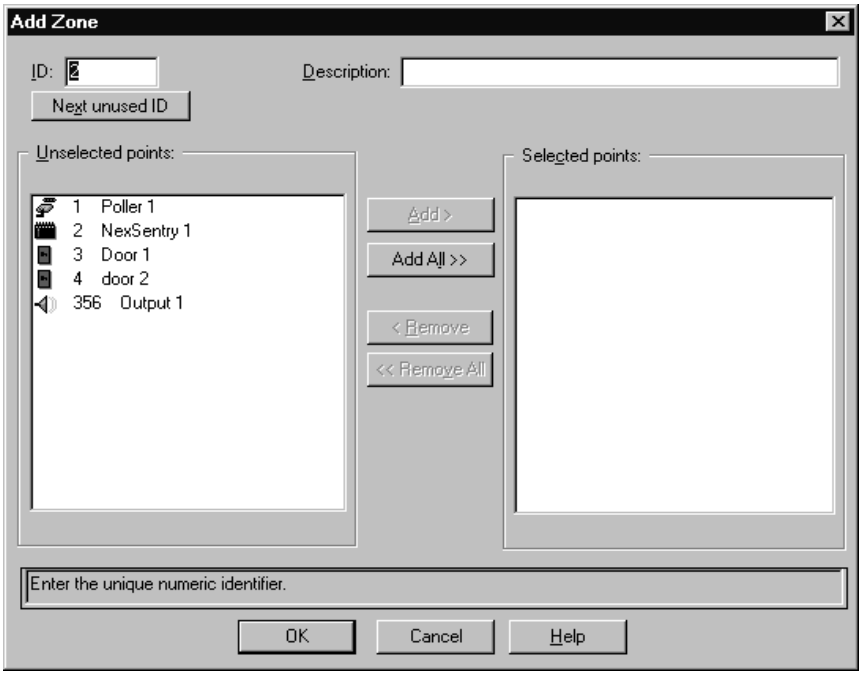
A Zone is any logical grouping of hardware elements that is determined by the NexSentry Manager system owner to increase efficiency. Placing hardware elements in zones can help you read or interpret system information quickly, and you can issue a single command that affects all device types within a zone.

Tip

A Zone could be all perimeter doors or all of the interior doors in one area of a building.

To view Zones:

1. From the Database menu, click **Browse**.
2. Double-click **Hardware** to expand its sub-entries.
3. Double-click **Zones**.
4. Click **Add.**



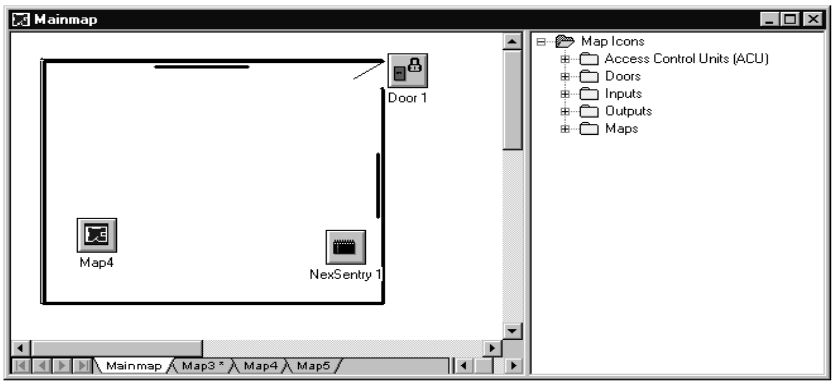
Add and Edit Zones Dialog Box

5. Enter data into each field as appropriate for Zones by referring to the completed data forms.
6. To save your changes and exit the Add Zones dialog box, click **OK**. The view Zones dialog box returns with your entry on the record list.

Maps

Maps allow you to graphically view information quickly. You can view different maps depending on the device type you select. The View Maps window allows you to operate the device type much in the same way as you would from the status menu.

You can create a Master Map that will encompass the entire secured area and incorporate smaller maps so that you can see more detail. Consult with your Installer for any maps or sketches that may have been made during the installation of the hardware for reference. After you have planned your map layout, proceed by making the various background files. These are graphic files that illustrate the building layout. In building the Map, you will place icons representing individual devices that you have previously installed on the system on these background files.



Map Window

Map Tool

The Maps feature can be accessed by choosing the Map tool from the toolbar.

To create a map, you must first draw the map using a graphics program. The Paint program in the Accessories folder of Windows NT will produce a Windows Bitmap file that will import directly into the NexSentry Manager. The NexSentry Manager supports many other graphics formats, such as Windows bitmaps (*.bmp), JPEG images (*.jpg), GIF images (*.gif) and more.

To create a map:

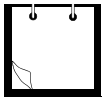
1. Click the Map Tool Icon.
2. Select **New** from Map in the main menu. You can also right-click to bring up the **Maps** menu.

Tip

*When you are creating a map for the first time, it will automatically be "**Map1.**" Each subsequent map will be named **"Map2"** or "**Map3**" and so on. You can use the default names or select **Rename** in the **Map** menu to change to a more descriptive name.*

3. Now that you have created and named the Map, you need to import your background file for the map.
4. On the Map menu, click Select Background. The Open file dialog box will appear, allowing you to select a background file.
5. Choose the background file for the map you are creating.
6. On the right side of the map window you will see a list of all the various hardware devices that you have installed in the system.
7. Expand the tree in order to display the last level. Select the hardware item you are mapping.
8. Drag the hardware item to the map area and place it where it belongs on the map background. To continue adding hardware to the map, repeat steps 7 and 8.

Note



You can only add icons for devices that you have defined. You must first add a new component through the add dialog box for that device in order for it to display on the list of available icons.

9. When you are finished, click **Save** from the Map menu.

Tip

From a Map, you can view system status for any device on the map. Right click on a map icon to bring up the status menu.

You can move an icon on the map by clicking on it and moving it where you want it to be.

*You can lock the icon in place by right-clicking and selecting **Lock Icon**.*

Chapter 4
Cardholder Data

Chapter Overview

This chapter covers how and when cardholders will be able to have access to the building. The first thing that you need to determine is when people or groups of people will have access. After setting up all of the access codes, you can assign individual cardholders.

- Configuring Access Codes Page 4-2
- Configuring Cardholders Page 4-4

Key Terms

- **Access Codes:** *A code assigned to cardholders to control where and when they are granted access. An Access Code consists of a door or a set of doors and a Time Group for each door.*
- **Cardholders:** *An employee, visitor, contractor, or individual who has a security card for the access control system.*
- **Door:** *In an access control system, the term "door" refers to any point of entry and all of its associated monitors and devices. A "door" may be a typical door, a gate, a corridor, a turnstile, an elevator, or any other area where people or vehicles might pass.*

Configuring Access Codes

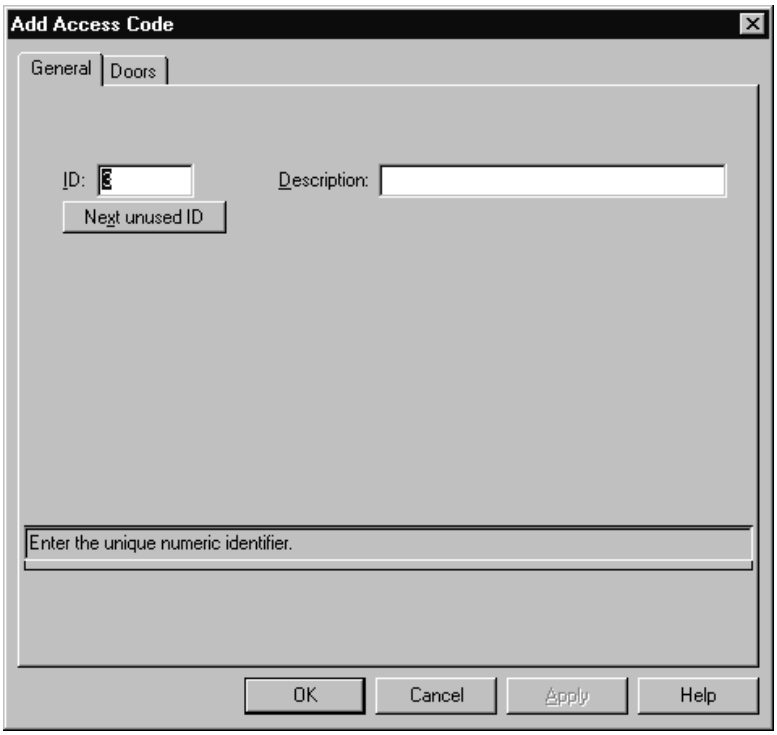
Access codes are a combination of Doors and Time Groups assigned to Cardholders to indicate where and when they are permitted access. Access codes can have an unlimited number of doors assigned to them, with one time group for each door or set of doors. There is only one access code assigned to each Cardholder.

To add an Access Code:

1. From the Database menu, click **Add**.
2. Click **Access Codes.**

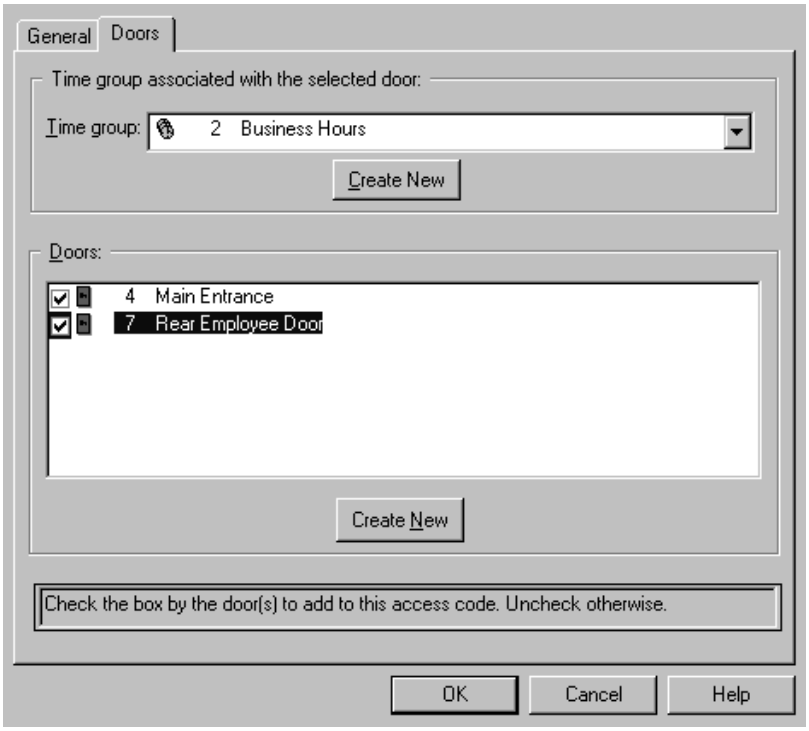
There are two pages to the Add and Edit Access Codes dialog box:

- General
- Doors



Add and Edit Access Codes Dialog Box

3. Enter data into each field as appropriate for access codes by referring to the completed data forms.



Add and Edit Access Codes "Door" Dialog Box

Note

When you are selecting doors, you must first select a Time Group and then you must select at least one door associated with that Time Group. Select the door by clicking the box next to the door icon.

Example: Door 1 is used with the Time Group that allows 24 hour access, while Door 2 can only be used during normal business hours. Choose the 24 hour Time Group and select Door 1. Next, choose Door 2, and then select the Time Group for Normal Business Hours.

4. To save your changes and exit the Add Access Codes dialog box, click **OK**. The view Access Codes dialog box returns with your entry on the record list.

Tip

*You can also access this dialog box by selecting it through the Browse Database option. There is also a keyboard shortcut by pressing **Ctrl-A** at the NexSentry Manager Main Window.*

Configuring Cardholders

Cardholders are individuals such as an employee, visitor, or contractor who has a security card for the access control system.

To add a Cardholder:

1. From the Database menu, click **Add**.
2. Click **Cardholder**.

There are seven pages to the Add and Edit Cardholder dialog box:

- General
- Access
- Credentials
- Address
- Additional Text Fields
- More Additional Text Fields
- Additional Look-up Fields

Add and Edit Cardholder Dialog Box

3. Enter data into each field as appropriate for access codes by referring to the completed data forms.

4. To save your changes and exit the Add Cardholders dialog box, click **OK**. The view Cardholders dialog box returns with your entry on the record list.

Tip

*You can also access this dialog box by selecting it through the Browse Database option. There is also a keyboard shortcut by pressing **Ctrl-K** at the NexSentry Manager Main Window.*

To view and edit Cardholders:

1. From the Database menu, click **Browse**.
2. Double-click **Personnel** in the Database outline to expand its sub-entries.
3. Click **Cardholders**, and then click **Edit**.
4. Select a cardholder(s) and make desired changes.
5. Do one of the following:

    a. To save your changes and exit the View Cardholders Dialog Box, click **OK**.

    b. To continue viewing cardholders, repeat steps 4 and 5.
6. Click **Close** to return to the Browse Database dialog box.

Tip

*If you are logged in the client with administrator privileges, you can view the PIN codes for each individual cardholder. From the View Cardholders dialog box, click **Records.** You can choose to view individual PIN codes or to print a PIN code report.*

Chapter 5
Using NexSentry Manager

Chapter Overview

Now that you have set up your Database, you are ready to use the NexSentry Manager!

This chapter will help with the daily tasks of monitoring and maintaining the NexSentry Manager and the Database.

- Monitoring Current Transactions Page 5-2
- Viewing the Transaction Log Page 5-5
- Working With Alarms Page 5-8
- Checking System Status Page 5-10
- Using Maps Page 5-14
- Backing Up the System Page 5-15

Key Terms

- **Shunt:** *A command issued to ignore a device or its messages. Example: Ignore messages from an open door when workers are moving furniture in and out of a building.*
- **Unshunt:** *A command issued to restore the device to normal.*
- **Monitor Window:** *Window for viewing transactions (or "events") on the system as they occur.*
- **Status Window:** *Window for viewing and changing device status for hardware on the system.*
- ***Transactions:*** *The individual events that occur in the access control system. It can be as simple as "Access Granted" when somebody uses their card, or an Alarm signaling a break-in.*

Monitoring Current Transactions

The NexSentry Manager is capable of monitoring the current activity of the entire system in “real time”—you can view transactions as they are occurring. This includes status of individual devices on the system.

Using the Monitor Window

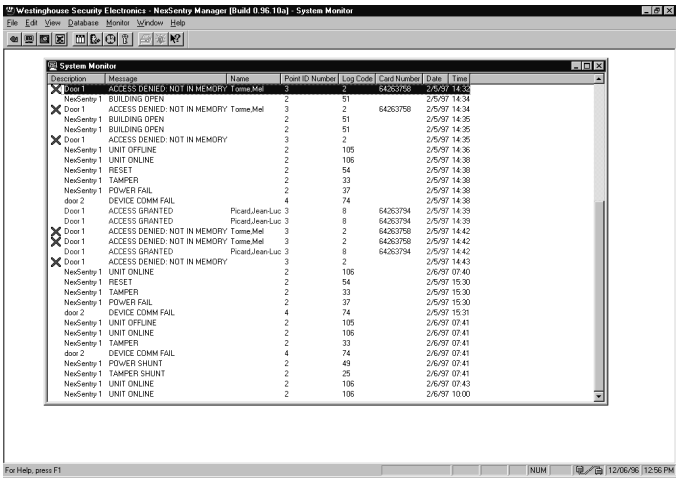
The Monitor window provides date, time, and access information about cardholder, device, and door activity.

To open the Monitor window:

System Monitor Tool

1. From the View menu, select **Monitor** (or click the **System Monitor Tool** in the Toolbar).
2. A Monitor window with the Monitor menu appears.

.


Westinghouse Security Electronics - NexSentry Manager [Build 0.96.10a] - System Monitor
File Edit View Database Monitor Window Help
System Monitor
Description Message Name Point ID Number Log Code Card Number Date Time
For Help, press F1
NUM
12/06/96 12:56 PM

Monitor Window

Tip

*You can access options by highlighting the desired transaction and **right-clicking** the mouse. This will bring up the options pull down menu for the highlighted transaction.*

The Monitor Menu

The Monitor menu is available only when you have the Monitor window open.

From the Monitor menu, you can check the status of the items in the Monitor window, service an alarm, clear the data from the window, activate or deactivate the scroll lock and perform the AutoFit function.

The Monitor menu adds two more items to the main menu, **Monitor** and **Window**:

- The **Monitor** selection in the menu allows you to change the status of hardware or to service an alarm.
- The **Window** selection is a standard Windows NT option allowing you to control the appearance of the screen.

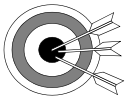
Viewing Recent Transactions

Activating the Monitor window allows you to see the most recent transactions. Icons can be selected to represent transaction types, and the icons will be displayed at the beginning of each line for those transactions. You can customize highlighting and text color to identify different transaction types.

Sorting Transactions

You can view the transactions chronologically, or sort by any field in the window. To sort by a particular field, simply click on the column header.

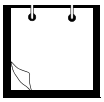
Example



To sort the Description in either descending or ascending order:

1. Click on the **Description** column header, and the Monitor window will sort all of the transactions by description in descending order, or in this case, reverse alphabetical order.
2. Click again on the Description column header and the Monitor window will sort the transaction descriptions alphabetically.You can sort all of the Monitor Window columns in this manner.

Note



The number of transactions allowed in the Monitor window is determined in the System Defaults dialog box. When the transaction number reaches the number set as the maximum number, the transaction will be "pushed off" the Monitor window and can only be viewed on the transaction log. The screen refresh time slows with a large number of transactions. You can change this number if desired, see *"System Defaults," Page 2-27*.

Viewing the Transaction Log

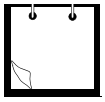
The transaction log stores all of the transactions on the system. This includes all of the transactions from the Monitor window and those transactions pushed off the Monitor window.

To view the Transaction Log:

Browse Tool

1. From the Database menu, click **Browse** or select the Browse tool.
2. Double-click **System Administration** in the Database outline to expand its sub-entries.
3. Click **Transactions** to expand its sub-entries: Log and Types.
4. Double-click **Log**. The transaction log appears.

Note



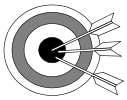
The value set in the System Default menu will determine the total number of transactions that will appear on the Monitor window. You can change this number if desired, see below.

Changing Transaction Defaults

Transactions are initially defined according to the settings in the default Database supplied with the NexSentry software. The NexSentry Manager links log codes (the codes sent by the ACUs) to the corresponding Transaction Type for display in the System Monitor window and storage in the Database.

In the Transactions Type Edit dialog box, you can customize each transaction or return the transaction to the default settings. This is also the dialog box that will allow you to control where the transaction is recorded, either on the hard drive or the printer, or both.

Example



For instance, if the description for log code 24 is “Door Forced,” you may want to change the description to read “Break-In.” Most of the default settings are quite descriptive of the code, but you can customize the system to better reflect your needs and situation.

To view or edit individual transactions:

Browse Tool

1. From the Database menu, click **Browse** or select the **Browse Tool**.
2. Double-click **System Administration** in the Database outline to expand its sub-entries.

3. Click **Transactions** to expand its sub-entries: Log and Types.
4. Double-click **Types** to display the Transaction Type dialog box.
5. Select a transaction and make desired changes.
6. Do one of the following:

    a. To save your changes and exit the View Transactions window, click **OK**.

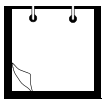
    b. To continue viewing and/or editing transactions, repeat steps 4 and 5.
7. Click **Close** to return to the Browse Database window.

Archiving

Because of the great number of total Transactions, the Transaction Log and the Audit Trail will become very large. In order to manage all of this information, you may want to archive the data periodically.

Archiving saves the system data from either the Transaction Log or the Audit Trail in a separate file. This allows you to remove historical data from the system and still have that information readily accessible. It also keeps the hard disk from filling up.

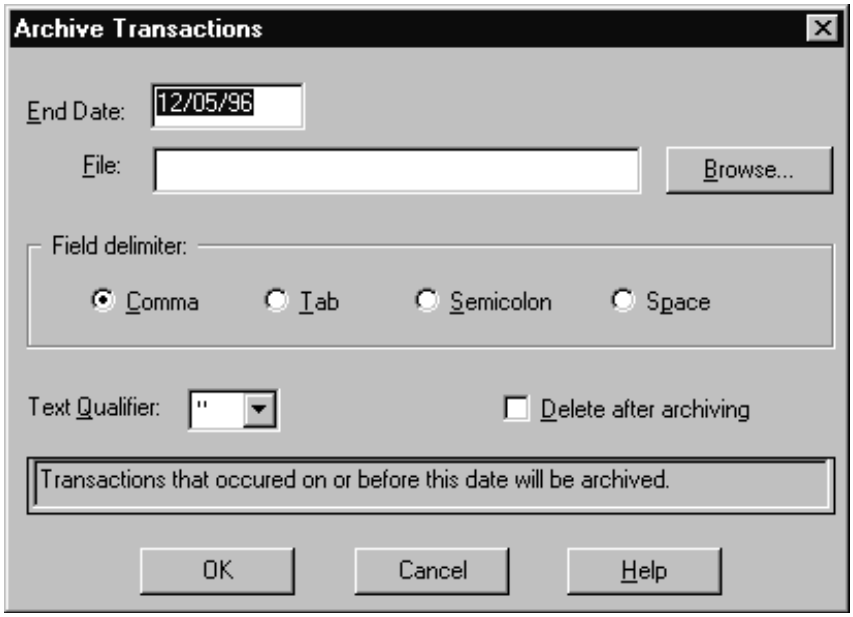
Note



*Archived **Transaction** files are a record of cardholder and system activity histories. Archived **Audit Trail** files are a record of all system user activity, such as adding hardware or Cardholders.*

To archive Transactions or Audit Trail:

1. From the Database menu, click **Archive Transactions** or **Archive Audit Trail**. The Archive Dialog Box will appear.
2. Enter Date and File information.



Archive Dialog Box

Tip

The Archived File is a simple text file that can be used by word processors and spreadsheets. You can select the field delimiter and the text qualifier based on the program you will be using for the Archive data.

If you want the archived Transactions deleted from the Transaction Log, check the "Delete after archiving" box.

3. Click **OK** to archive file and return to the Database menu.

Note

In addition to archiving to save data, you should also use a Backup program to save your important data. Archiving does not save Hardware or Cardholder information. See "Backing Up the System," Page 5-15.

Working With Alarms

An alarm can be set so that when a specified event occurs anywhere in the system, it will alert the security personnel monitoring the system.

Viewing Alarms

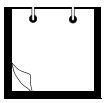
When an alarm sounds, the alarm service icon appears in the Status Bar as well as a Transaction in the Monitor Window. In order to service an Alarm, you must open the Alarm Servicing window. From this window, the operator may acknowledge the alarm, mark it as read, call up the ACU status or the individual device status.

To view alarms:

Alarm Tool

1. From the Main menu, click **View**, then **Alarm** (or click the **Alarm Tool** from Toolbar).
2. The Alarm Service window appears; from this window, you can acknowledge the alarm or call up the ACU or individual device status.
3. Click on the transaction that has triggered the alarm.
4. Right-click to display the Alarm Service menu.
5. Select **Acknowledge**, or **ACU Status**, or **Show Status**.

Note



See "Checking System Status," Page 5-10 for details on System Status.

Acknowledging and Silencing Alarms

You can acknowledge an alarm by selecting **Acknowledge** in the Alarm menu, or right-clicking the mouse on the alarm. On the Acknowledge Alarm Dialog box, you can enter a response to the alarm and either mark the alarm as having been read, or clear the alarm from the Alarm Servicing window.

Silence Tool

You can also turn off the audio alarm by selecting the Silence tool. It will not acknowledge or clear the alarm, but it will stop the sound.

By silencing the alarm you can turn off the audio alarm. The transaction that caused the alarm will still be active in the Alarm Service window.

Tip

You can also acknowledge alarms by right-clicking on the alarm icon in the Status bar.

You can service multiple alarms by selecting more than one, and then choosing the selection in the Alarm menu.

Checking System Status

System Status windows give an overall dynamic view of your access control system's status. A Status window provides the current status and setting for each monitoring point. From Status windows, you can check the following:

- System components and equipment security.
- Building/Sector modes (open, limited, or closed).
- Doors and monitors.

Viewing Status Windows

Unacknowledged alarms are shown in the Status bar at the bottom of the screen. Status windows can be sorted according to your needs and you can open up more than one at a time.

To view the Status Window for a device:

1. From the Main menu, click **View**.
2. Select device type (such as Poller or ACU).
3. The Status window for the device appears.

Filtering Status Window Data

You can filter the Status window and display only a particular type of device from a specific zone. This can help reduce the quantity of information viewed at one time to a more manageable level.

To filter Status window data:

1. From the Main menu, click **View**.
2. Select **Status,** and then **Status Filter**. The Status Filter dialog box appears.

Status Tool

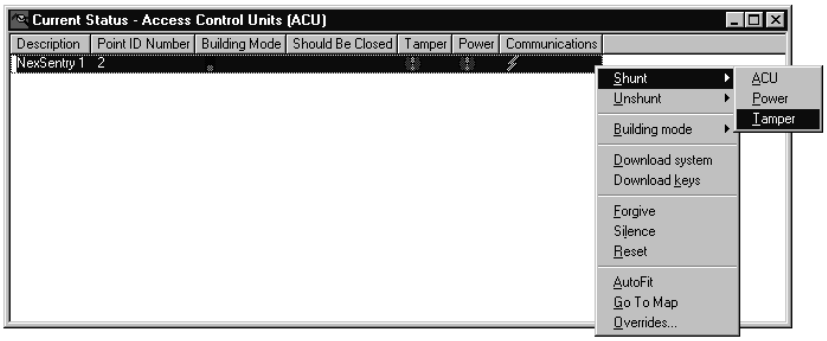
You can also click the Current Status tool in the Toolbar to access the Status Filter dialog box.

Activating the Status Menu

Like the Monitor menu, the Status menu is only visible when you are in a Status window.

To activate the Status menu:

1. From the active Status window, select the transaction you wish to view.
2. From the Main menu click **Status**, or right-click the mouse.
3. The Status menu for the device appears.



Status Window with the Status menu displayed

The Status menu will vary with the unique properties of each device. All of the devices have the ability to shunt/unshunt, and some have options as to which element to shunt/unshunt. For example, the ACU can shunt/unshunt the device itself, the power messages, or the tamper messages.

See Tables 5-1 through 5-5 for the Status menu options of the various devices:

Table 5-1. Pollers

Status Menu Options	Description
Shunt	Shunt the Poller
Unshunt	Unshunt the Poller

Table 5-2. ACUs

Status Menu Options	Sub menu option	Description
Shunt	ACU Power Tamper	Shunt the device Shunt the power messages from this point shunt the tamper messages from this point
Unshunt	ACU Power Tamper	Unshunt the device Unshunt the power messages from this point Unshunt the tamper messages from this point

Table 5-2. ACUs [continued]

Status Menu Options	Sub menu option	Description
Building Mode	Open Limited Closed	Set the building mode to “Open” Set the building mode to “Limited” Set the building mode to “Closed”
Download System	N/A	Download System Database to this ACU
Download Keys	N/A	Download Cardholder Database to this ACU
Forgive	N/A	Forgive Allows the operator to Forgive when Anti-Passback is used
Silence	N/A	Silence the alarm
Reset	N/A	Allows the operator to Reset the ACU.
AutoFit	N/A	Adjust the column widths to be only as wide as the column contents
Go To Map	N/A	Display the Maps window
Overrides	N/A	Allows multiple commands to be applied to the selected ACU(s)

Table 5-3. Doors

Status Menu Option	Submenu Options	Description
Shunt or Unshunt	Door Coax MSM Analog Reader VIP VIP Tamper Digital Reader Digital Reader Tamper	Shunt this door Shunt all coax messages for this point Shunt all Multiple Switch Monitor messages Shunt all Sensor messages Shunt the Keypad Shunt the Keypad tamper Shunt the Digital Reader (SCR/DR) Shunt the Digital Reader tamper
Unshunt	Door Coax MSM Analog Reader VIP VIP Tamper Digital Reader Digital Reader Tamper	Unshunt this door Unshunt all coax messages for this point Unshunt all Multiple Switch Monitor messages Unshunt all Sensor messages Unshunt the Keypad Unshunt the Keypad tamper Unshunt the Digital Reader (SCR/DR) Unshunt the Digital Reader tamper
Lock	N/A	Lock the door
Unlock	N/A	Unlock the door

Table 5-3. Doors [continued]

Status Menu Option	Submenu Options	Description
Timed Unlock	N/A	Unlock the door with automatic timed lock/unlock
AutoFit	N/A	Adjust the column widths to be only as wide as the column contents
Go To Map	N/A	Display the Maps window
Override	N/A	Allows multiple commands to be applied to the selected door(s)

Table 5-4. Outputs

Status Menu Options	Description
Shunt	Shunt the output
Unshunt	Unshunt the output
Activate	Activate the output
Deactivate	Deactivate the output
Go To Map	Display the Maps window

Table 5-5. Inputs

Status Menu Options	Description
Shunt	Shunt the input
Unshunt	Unshunt the input
Go To Map	Display the Maps window

Tip

You can select multiple devices and make the same changes. For example, you could select all of the doors in one area or zone and unlock them all at one time.

Using Maps

Maps allow you to graphically view information quickly. Basic status will be shown on the map icons that represent each type of hardware component.

To view Maps:

1. Click on the Map Tool from Toolbar. The Map window displays.
2. On the viewing side of the Map window, click on the name of the map you wish to view.

To change the Status of a device on the Map:

1. Place the pointer on the device and right-click. The Status menu for that device will appear.
2. Select the menu item.

   or

   Select another icon.

See "Maps," Page 3-17, for details on creating or modifying maps.

Backing Up the System

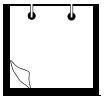
You have spent a great deal of time creating the Database, so you will want to back up your work. You should back up the NexSentry Manager system:

- When you have finished initial data input.
- Periodically during normal operation.

There are several backup methods that you can use, such as daily, weekly, multiple copies, or incremental. A good backup plan will ensure you do not lose valuable data.

You should use the backup and restore capabilities of Window NT to maintain your system.

Note



Refer to the Windows NT Reference for using Backup.

The most important file is the ".mdb" file. This is the file that will store all the information that you entered about your system.*

Chapter 6
Troubleshooting

Chapter Overview

This chapter covers some of the most frequently encountered problems and typical solutions. These problems are presented in the form of conditions and then followed by questions that you can answer that will lead you to a solution.

- Troubleshooting Questions Page 6-2
- Error Messages Page 6-5

Key Terms

- **Client:** *A computer that requests the service of another computer. A workstation requesting the contents of a file from a file server is a client of the file server.*
- **Server:** *A computer which, by means of network connections, carries out parts of a computing task on behalf of one or more remote computers. The computer where the NexSentry Manager Database is located is the NexSentry Server.*

Troubleshooting Questions

The NexSentry Manager installation program will not run.

Q. Is the CD-ROM drive working properly?

A. Check in Windows NT Control Panel.

Q. Is the drive properly labeled? Is it drive “d” or some other letter?

A. Make sure that you are properly identifying the drive.

Q. Are you logged on as the Administrator or with Administrator functions?

A. Some log on accounts in Windows NT will not allow you to copy and install files. If this is the case, you should get Administrator privileges or log on as the Administrator.

The NexSentry Manager is installed but will not run.

Q. Does the computer system meet the System Requirements? See “System Requirements,” Page 1-2.

A. Try Restarting Windows NT and then running the NexSentry Manager.

The NexSentry Manager will not communicate with the server.

Q. Is the IP address you used during the installation correct?

A. You could run the installation program again to ensure that your network information is correct. Before doing this, make a back-up copy of the Database to save the data you have already entered.

You should also check to make sure that the Network server that you are using assigns the same IP address each time you log on. If your server uses DHCP and assigns an IP address, contact your administrator to get a dedicated IP assignment.

The NexSentry Manager will not communicate with the ACU and the associated devices.

Q. Are the ACUs Addressed? See “Addressing ACUs,” Page 3-5.

A. Ensure that when you have addressed the ACUs that you type “Reset” when finished in order to save the information and update the ACU.

Q. Are the ACU addresses correct?

A. Each ACU must be uniquely numbered numbered. Consult with your installer and the NexSentry Manager Input Forms for the correct address.

Q. Are the COM Ports working?

A. The installer may be able to test the COM Ports to ensure that they are working properly.

Q. Do you have the Poller for that ACU installed?

A. The ACU must have a Poller installed and properly defined in the NexSentry Manager in order to communicate with the ACUs. Ensure that you have properly installed the Poller according to the Input Forms.

Q. Are all of the serial cables connected correctly and securely?

A. Check to make sure that all of the cables are securely connected to the right connectors on your computer.

Q. Does the address in the Add or Edit ACU Dialog Box match the ACU address that you set using Hyperterminal?

A. You must make certain that the Address you gave the ACU when you configured it directly in Hyperterminal is the same as the one you assign it in the NexSentry Manager.

Cards and Cardholders are in the Database but still can't get access.

Q. Has the information been downloaded to the ACUs?

A. Check the System Default menu for download times and if the "download on discrepancy" is checked. You might also remember to manually download the information to the ACUs after you have input new Cards or Cardholders. Select the Download system or Download keys to update the ACU's for any changes you have made.

Q. Is the Access Code defined correctly?

A. Check the Access code definition for the Card and compare with the door requiring the access.

Q. Is the Start Date correct?

A. Check the Start Date in the Access page of the Add or Edit Cardholder Dialog Box.

Error Messages

The following table lists the most common error messages

Table 6-1. NexSentry Client Error Messages

When it occurs	Messages	Comments
Adding (or modifying) poller with a used port number (COM1 etc).	The poller 'Port' you have specified is already used by the following poller: Please change the 'Port' and try again.	Assign another available port.
Adding (or modifying) ACU with a used Poller/Address combination.	The 'Address' you have specified is already used by the following ACU. Please change the 'Address' and try again.	Verify that the address for the ACU you are assigning is correct.
Adding (or modifying) Door with a used ACU/Sensor combination.	The 'Sensor' you have specified is already used by the following Door. Please change the 'Sensor' and try again.	Verify that the sensor you are assigning is correct.
Adding (or modifying) Input or Output with a used ACU/Sensor/Contact combination.	The 'Sensor/Contact' you have specified is already used by the following record. Please change the Sensor and/or Contact and try again.	Verify that the Input or Output you are assigning is correct.
Deleting a record when items referencing it still exist.	Can't delete or change record. It is in use by a record of type.	Can’t delete an ACU if it is included in a zone, a door or any other device’s definition.
When a non-existent item is selected from a combo box.	Can't add or change record. Referenced record of type “X“ does not exist. It could have been deleted by other users, or lost because of an error during a previous operation.	Verify that the item is defined in the system.

Table 6-1. NexSentry Client Error Messages

When it occurs	Messages	Comments
During application initialization.	Database is secured for read only access. Continue anyway?	Contact Administrator.
If Add/Modify is attempted with a read-only database.	Operation failed. Database is secured for read only access.	Contact Administrator.
Adding (or modifying) a record with a used ID.	The ID you have entered is already used by the following record, “X.” Please change the ID and try again. Click “Next unused ID” button to find the next available ID.	Click “Next unused ID” button to find the next available ID.
Adding (or modifying) a record with an ID used up by a record. Record is of different type but shares the set of IDs.	The ID you have entered is already used by another record. Please change the ID and try again. Click “Next unused ID” button to find the next available ID.	All of the hardware items will have unique number IDs.
During application initialization.	Can't open database connection.	Verify network communication with server. See “Troubleshooting Questions,” Page 6-2.
Client/server communication breakdown	Lost connection to the server. Either the server or the network could be having problems. If the connection is not restored for a long time, quit and restart the client.	Try clicking the communication icon to reconnect to the server. See “Troubleshooting Questions,” Page 6-2.
Unable to establish client/server communication.	Could not establish communication with the server. Either the server or the network could be having problems.	See “Troubleshooting Questions,” Page 6-2.

Appendix A

NexSentry Manager Input Forms

This section contains copies of the NexSentry Manager Input forms. The forms may be used as master copies to make the input forms for installation use.

The forms are organized by their sequence in the installation process.

Note

See chapter 1 for more information on using the forms for the initial setup of your database.

Pollers

ID	Description	Instruction	Show Activity Times
Host Port	Host Baud	Acknowledge Timeout Seconds	Retries

ID	Description	Instruction	Show Activity Times
Host Port	Host Baud	Acknowledge Tim-eout Seconds	Retries

ID	Description	Instruction	Show Activity Times
Host Port	Host Baud	Acknowledge Tim-eout Seconds	Retries

ID	Description	Instruction	Show Activity Times
Host Port	Host Baud	Acknowledge Tim-eout Seconds	Retries

ID	Description	Instruction	Show Activity Times
Host Port	Host Baud	Acknowledge Tim-eout Seconds	Retries

Inputs

ID	Description	Instruction	Show Activity Times	Action
ACU	Shunted	ACU Port No.	Contact No.	

ID	Description	Instruction	Show Activity Times	Action
ACU	Shunted	ACU Port No.	Contact No.	

ID	Description	Instruction	Show Activity Times	Action
ACU	Shunted	ACU Port No.	Contact No.	

ID	Description	Instruction	Show Activity Times	Action
ACU	Shunted	ACU Port No.	Contact No.	

ID	Description	Instruction	Show Activity Times	Action
ACU	Shunted	ACU Port No.	Contact No.	

Outputs

ID	Description	Instruction	Show Activity Times	Action
ACU	Shunted	ACU Port No.	Contact No.	

ID	Description	Instruction	Show Activity Times	Action
ACU	Shunted	ACU Port No.	Contact No.	

ID	Description	Instruction	Show Activity Times	Action
ACU	Shunted	ACU Port No.	Contact No.	

ID	Description	Instruction	Show Activity Times	Action
ACU	Shunted	ACU Port No.	Contact No.	

ID	Description	Instruction	Show Activity Times	Action
ACU	Shunted	ACU Port No.	Contact No.	

Instructions

ID	Description	Instruction

System Users

ID	Description	Security Level	User Name	Password
Example	John Doe	2	Jdoe	HR2056P
1				
2				
3				
4				
5				
6				
7				
8				
9				
10				
11				
12				
13				
14				
15				
16				
17				
18				
19				
20				

ACU Users

ID	Description	Rank (A-F)	User Name	Password
Example	John Doe	A	JohnD	Decartes
1				
2				
3				
4				
5				
6				
7				
8				
9				
10				
11				
12				
13				
14				
15				
16				
17				
18				
19				
20				

Time Codes

ID	Description	Start Time	Stop Time	Sun	Mon	Tues	Wed	Thu	Fri	Sat	Holi-day	Time Groups
	AM Shift -Example-	0800	1630		x	x	x	x	x			
1												
2												
3												
4												
5												
6												
7												
8												
9												
10												
11												
12												
13												
14												
15												
16												
17												
18												
19												
20												

ACU

Table 0-1. General

ID	Description	Poller	Instruction	Minutes between reminder messages

Table 0-2. Time Groups

Time Groups	Times when building should be closed	Show Activity Times

Table 0-3. VIP

VIP Enable	Retries	Digits	Digits if VIP only	Pin Seed	Grace Period	Duress

Table 0-4. Actions

System	Operator Override	Duress	Tamper	Power Fail

Table 0-5. Cards

Card Type	Facility Code	Alternate Code
1030 1040 1050 1060D		

Table 0-6. Reader

Verification Sweeps	Misread Filter	Access Time Denied	Reread Delay

Table 0-7. Misc.

Host Baud	Xon/Xoff	Terminal Baud	Xon/Xoff

Doors

Table 0-8. General

ID	Description	ACU	Shunt	Sensor Number

Table 0-9. Time Groups

Auto Unlock	Show Activity Times

Table 0-10. Lock

Use Door Switch	Contact Point	Max Door Open Time	Read Cards While Open	Unlock Time	Reverse Lock
					Yes No

Table 0-11. Proximity Reader

Enable	Type	Used As	Disable MSM
	Digital Analog SCR	Normal Open Closed Station	Yes No

Table 0-12. VIP

VIP Enable	Active During Modes	During Timegroup
Yes No	Open Limited Closed	

Table 0-13. REX (Request to Exit)

Enable	Contact Point	Valid REX Timegroup	Unlock on ReX
			Yes No

Table 0-14. Misc.

Anti Passback	Method	Type	Instruction	Action Group
Enable	Hard Soft	Enter Exit		

Cardholders

Table 0-15. General

ID	First	Middle	Last

Table 0-16. Access

Options	Dates	Code
Trace Visitor Privileged	Start Stop	

Table 0-17. Credentials

Card type	Facility Code	Card Number	PIN

Table 0-18. Address

Line 1	Line 2	Line 3

Table 0-19. Additional Text Fields (1-4)

1	2	3	4

Table 0-20. Additional Text Fields (5-8)

5	6	7	8

Table 0-21. Additional Lookup Fields (1-6)

1	2	3
4	5	6

Security Level

Security Level #_____

		Device
View	Edit	Pollers
View	Edit	ACUs
View	Edit	Doors
View	Edit	General Purpose Inputs
View	Edit	Door Switch Input
View	Edit	REX Input
View	Edit	Outputs
View	Edit	Instructions
View	Edit	Zones
View	Edit	Cardholders
View	Edit	Access Codes
View	Edit	System Users
View	Edit	Security Levels
View	Edit	ACU Users
View	Archive	Transaction Log
View	Edit	Transaction Types
View	Edit	Alarm Responses
View	Archive	Audit Trail
View	Edit	Additional Lookup Fields
View	Edit	Additonal Text Fields
View	Edit	Facility Codes
View	Edit	Time Codes

		Device
View	Edit	Time Groups
View	Edit	Holidays
View	Edit	Actions
View	Edit	Action Groups
View	Edit	Maps
View	Edit	Sounds
View	Edit	System Defaults
View		Status
View		Monitor
View	Ackn.	Clear Alarms
Shunt/Unshunt		ACU
Change		Building Mode
Download		System Data
Download		Cardholders
		Forgive
		Silence
		Reset
Shunt/Unshunt		Doors
Lock/Unlock		Doors
Shunt/Unshunt		Pollers
Shunt/Unshunt		Inputs

Alarm Responses

ID	Alarm Response	Comments

Facility Codes

ID	Description	Code

Appendix B

NexSentry Manager Database File Structure

Objec	Name	Field Type	Si
Table	tblAccessCodeDescriptions		
Colum	AccessCodeDescriptions_nAccessCod	Number	2
Colum	AccessCodeDescriptions_sDescription	Text	30
Table	tblAccessCodes		
Colum	AccessCodes_nAccessCode	Number	2
Colum	AccessCodes_lPointID	Number	4
Colum	AccessCodes_nTimegroupID	Number	4
Table	tblActionGroups		
Colum	ActionGroups_lActionGroupsID	Number	2
Colum	ActionGroups_sDescription	Text	30
Colum	ActionGroups_nKeyTrace	Number	2
Colum	ActionGroups_nAccessGranted	Number	2
Colum	ActionGroups_nAccessDenied	Number	2
Colum	ActionGroups_nDoorOpenTooLong	Number	2
Colum	ActionGroups_nDoorForcedOpen	Number	2
Colum	ActionGroups_nCoaxFailure	Number	2
Colum	ActionGroups_nSensorFailure	Number	2
Colum	ActionGroups_nMSMFailure	Number	2
Colum	ActionGroups_nExitGranted	Number	2
Colum	ActionGroups_nExitDenied	Number	2
Colum	ActionGroups_nVIPFailure	Number	2
Colum	ActionGroups_nVIPSCRDRFailure	Number	2
Colum	ActionGroups_nDoorsDeviceTamper	Number	2
Colum	ActionGroups_nSNETReaderFailure	Number	2
Colum	ActionGroups_nABACardAction	Number	2
Table	tblActions		
Colum	Actions_nActionID	Number	2
Colum	Actions_sDescription	Text	30
Colum	Actions_bSendToHostClosed	Yes/No	1
Colum	Actions_bSendToHostLimited	Yes/No	1

Objec	Name	Field Type	Si
Colum	Actions_bSendToHostOpen	Yes/No	1
Colum	Actions_nSendToHostTimegroupID	Number	4
Colum	Actions_bCloseLatchedContactClose	Yes/No	1
Colum	Actions_bCloseLatchedContactLimited	Yes/No	1
Colum	Actions_bCloseLatchedContactOpen	Yes/No	1
Colum	Actions_nCloseLatchedContactTimegr	Number	4
Colum	Actions_lCloseContactPointID	Number	4
Colum	Actions_bCloseContactWhenClosed	Yes/No	1
Colum	Actions_bCloseContactWhenLimited	Yes/No	1
Colum	Actions_bCloseContactWhenOpen	Yes/No	1
Colum	Actions_nCloseContactTimegroupID	Number	4
Colum	Actions_bPreventBldgClose	Yes/No	1
Colum	Actions_bPrintAsterisk	Yes/No	1
Table	tblACUModemData		
Colum	ACUModemData_lPointID	Number	4
Colum	ACUModemData_sBanner1	Text	50
Colum	ACUModemData_sBanner2	Text	50
Colum	ACUModemData_sBanner3	Text	50
Colum	ACUModemData_sPhoneNumber1	Text	50
Colum	ACUModemData_sPhoneNumber2	Text	50
Colum	ACUModemData_sPhoneNumber3	Text	50
Colum	ACUModemData_bNumberCallingTrie	Number	1
Colum	ACUModemData_bCallback	Yes/No	1
Colum	ACUModemData_lDialThreshold	Number	4
Colum	ACUModemData_sModemInitString	Text	50
Colum	ACUModemData_sModemDialString	Text	50
Colum	ACUModemData_sModemHangupStri	Text	50
Colum	ACUModemData_lNoActivityTimeout	Number	4
Table	tblACUUsers		
Colum	ACUUsers_nUserID	Number	1
Colum	ACUUsers_sUserDescription	Text	30
Colum	ACUUsers_lPointID	Number	4
Colum	ACUUsers_sUserName	Text	12
Colum	ACUUsers_sPassword	Text	8
Colum	ACUUsers_bRank	Number	1
Table	tblAlarmResponses		
Colum	AlarmResponses_nAlarmResponseID	Number	2
Colum	AlarmResponses_sDescription	Text	60
Colum	AlarmResponses_sRemarks	Text	25

Objec	Name	Field Type	Si
Table	tblAlarms		
Colum	Alarms_lTransactionID	Number	4
Colum	Alarms_lPointID	Number	4
Colum	Alarms_lEmployeeID	Number	4
Colum	Alarms_nCredentialID	Number	2
Colum	Alarms_dTransactionLogDate	Date/Time	8
Colum	Alarms_tTime	Date/Time	8
Colum	Alarms_nTransactionType	Number	2
Colum	Alarms_bPriority	Number	1
Colum	Alarms_dAcknowledgeDate	Date/Time	8
Colum	Alarms_tAcknowledgeTime	Date/Time	8
Colum	Alarms_bACUUserID	Number	1
Colum	Alarms_bLoginID	Number	1
Colum	Alarms_sAlarmRemarks	Text	25
Colum	Alarms_bAlarmStatus	Number	1
Colum	Alarms_nAlarmResponseID	Number	2
Table	tblAudit		
Colum	Audit_lTranID	Number	4
Colum	Audit_lID	Number	4
Colum	Audit_sDescrip	Text	30
Colum	Audit_bAction	Number	1
Colum	Audit_sUname	Text	50
Colum	Audit_dDate	Date/Time	8
Colum	Audit_tTime	Date/Time	8
Table	tblCredentials		
Colum	Credentials_nCredentialID	Number	2
Colum	Credentials_bType	Number	1
Colum	Credentials_bCardType	Number	1
Colum	Credentials_bFacilityCode	Number	2
Colum	Credentials_lCredentialValue	Number	4
Colum	Credentials_lPINCode	Number	4
Table	tblDevice818SC		
Colum	Device818SC_lPointID	Number	4
Colum	Device818SC_nOperatorOverrideActio	Number	2
Colum	Device818SC_bTerminalPortXOnXOff	Yes/No	1
Colum	Device818SC_bHostPortXOnXOff	Yes/No	1
Colum	Device818SC_nTamperAction	Number	2
Colum	Device818SC_nPowerFailAction	Number	2
Colum	Device818SC_nFacilityCodeID	Number	2
Colum	Device818SC_nAlternateFacilityCodeI	Number	2

Objec	Name	Field Type	Si
Colum	Device818SC_bCardType1060	Yes/No	1
Colum	Device818SC_bCardType1050	Yes/No	1
Colum	Device818SC_bCardType1040	Yes/No	1
Colum	Device818SC_bCardType1030	Yes/No	1
Colum	Device818SC_nBldgShouldBeClosedT	Number	4
Colum	Device818SC_nBldgClosedReminder	Number	2
Colum	Device818SC_lTerminalPortBaudRate	Number	4
Colum	Device818SC_lHostPortBaudRate	Number	4
Colum	Device818SC_nPINSeed	Number	2
Colum	Device818SC_bPINGracePeriod	Number	1
Colum	Device818SC_bPINRetries	Number	1
Colum	Device818SC_nAccessDeniedTime	Number	2
Colum	Device818SC_bDuressEnable	Yes/No	1
Colum	Device818SC_bPrintIfVIPOnlyCard	Yes/No	1
Colum	Device818SC_bNumberOfPINDigits	Number	1
Colum	Device818SC_bVIPOnlyCardDigits	Number	1
Colum	Device818SC_nAutoForgiveTimegroup	Number	4
Colum	Device818SC_nDuressAction	Number	2
Colum	Device818SC_nRepeatedReadDelay	Number	2
Colum	Device818SC_bMisReadFilter	Number	1
Colum	Device818SC_bNumberOfSweeps	Number	1
Colum	Device818SC_lPollerPointID	Number	4
Table	tblDeviceNexSentry		
Colum	DeviceNexSentry_lPointID	Number	4
Colum	DeviceNexSentry_nOperatorOverrideA	Number	2
Colum	DeviceNexSentry_bTerminalPortXOnX	Yes/No	1
Colum	DeviceNexSentry_bHostPortXOnXOff	Yes/No	1
Colum	DeviceNexSentry_nTamperAction	Number	2
Colum	DeviceNexSentry_nPowerFailAction	Number	2
Colum	DeviceNexSentry_nFacilityCodeID	Number	2
Colum	DeviceNexSentry_nAlternateFacilityCo	Number	2
Colum	DeviceNexSentry_bCardType1060	Yes/No	1
Colum	DeviceNexSentry_bCardType1050	Yes/No	1
Colum	DeviceNexSentry_bCardType1040	Yes/No	1
Colum	DeviceNexSentry_bCardType1030	Yes/No	1
Colum	DeviceNexSentry_nBldgShouldBeClos	Number	4
Colum	DeviceNexSentry_nBldgClosedRemind	Number	2
Colum	DeviceNexSentry_lTerminalPortBaudR	Number	4
Colum	DeviceNexSentry_lHostPortBaudRate	Number	4
Colum	DeviceNexSentry_nPINSeed	Number	2
Colum	DeviceNexSentry_bPINGracePeriod	Number	1
Colum	DeviceNexSentry_bPINRetries	Number	1

Objec	Name	Field Type	Si
Colum	DeviceNexSentry_nAccessDeniedTim	Number	2
Colum	DeviceNexSentry_bDuressEnable	Yes/No	1
Colum	DeviceNexSentry_bPrintIfVIPOnlyCard	Yes/No	1
Colum	DeviceNexSentry_bNumberOfPINDigit	Number	1
Colum	DeviceNexSentry_bVIPOnlyCardDigits	Number	1
Colum	DeviceNexSentry_nAutoForgiveTimegr	Number	4
Colum	DeviceNexSentry_nDuressAction	Number	2
Colum	DeviceNexSentry_nRepeatedReadDel	Number	2
Colum	DeviceNexSentry_bMisReadFilter	Number	1
Colum	DeviceNexSentry_bNumberOfSweeps	Number	1
Colum	DeviceNexSentry_lPollerPointID	Number	4
Table	tblDevices		
Colum	Devices_lPointID	Number	4
Colum	Devices_bType	Number	1
Table	tblDoor818SC		
Colum	Door818SC_lPointID	Number	4
Colum	Door818SC_nActionGroupsID	Number	2
Colum	Door818SC_bSensorUse	Number	1
Colum	Door818SC_bAntiPassback	Number	1
Colum	Door818SC_bAntiPassbackType	Number	1
Colum	Door818SC_bReverseUnlock	Yes/No	1
Colum	Door818SC_nUnlockTimeLength	Number	2
Colum	Door818SC_nDoorOpenTooLongTime	Number	2
Colum	Door818SC_lDoorSwitchPointID	Number	4
Colum	Door818SC_lREXPointID	Number	4
Colum	Door818SC_bUnlockOnREX	Yes/No	1
Colum	Door818SC_nValidREXTimegroupID	Number	4
Colum	Door818SC_nAutoUnlockTimegroupID	Number	4
Colum	Door818SC_bReadCardWhileOpen	Yes/No	1
Colum	Door818SC_bSensorDisable	Yes/No	1
Colum	Door818SC_bMSMDisable	Yes/No	1
Colum	Door818SC_bVIPEnable	Yes/No	1
Colum	Door818SC_bVIPBldgModeOpen	Yes/No	1
Colum	Door818SC_bVIPBldgModeLimited	Yes/No	1
Colum	Door818SC_bVIPBldgModeClosed	Yes/No	1
Colum	Door818SC_nVIPTimegroupID	Number	4
Colum	Door818SC_bSCRDRReaderEnable	Number	1
Colum	Door818SC_bForwardDigitCode	Yes/No	1
Colum	Door818SC_bReadRange	Number	1
Colum	Door818SC_bNumberVerifyReads	Number	1
Colum	Door818SC_lVerifyTimeWindow	Number	4

Objec	Name	Field Type	Si
Colum	Door818SC_lBeeperOnDuration	Number	4
Colum	Door818SC_lBeeperOffDuration	Number	4
Colum	Door818SC_lBeeperOnOffDuration	Number	4
Colum	Door818SC_lRedLEDOnDuration	Number	4
Colum	Door818SC_lRedLEDOffDuration	Number	4
Colum	Door818SC_lRedLEDOnOffDuration	Number	4
Colum	Door818SC_lGreenLEDOnDuration	Number	4
Colum	Door818SC_lGreenLEDOffDuration	Number	4
Colum	Door818SC_lGreenLEDOnOffDuration	Number	4
Colum	Door818SC_lACUPointID	Number	4
Table	tblDoorNexSentry		
Colum	DoorNexSentry_lPointID	Number	4
Colum	DoorNexSentry_nActionGroupsID	Number	2
Colum	DoorNexSentry_bSensorUse	Number	1
Colum	DoorNexSentry_bAntiPassback	Number	1
Colum	DoorNexSentry_bAntiPassbackType	Number	1
Colum	DoorNexSentry_bReverseUnlock	Yes/No	1
Colum	DoorNexSentry_nUnlockTimeLength	Number	2
Colum	DoorNexSentry_nDoorOpenTooLongTi	Number	2
Colum	DoorNexSentry_lDoorSwitchPointID	Number	4
Colum	DoorNexSentry_lREXPointID	Number	4
Colum	DoorNexSentry_bUnlockOnREX	Yes/No	1
Colum	DoorNexSentry_nValidREXTimegroupI	Number	4
Colum	DoorNexSentry_nAutoUnlockTimegrou	Number	4
Colum	DoorNexSentry_bReadCardWhileOpe	Yes/No	1
Colum	DoorNexSentry_bSensorDisable	Yes/No	1
Colum	DoorNexSentry_bMSMDisable	Yes/No	1
Colum	DoorNexSentry_bVIPEnable	Yes/No	1
Colum	DoorNexSentry_bVIPBldgModeOpen	Yes/No	1
Colum	DoorNexSentry_bVIPBldgModeLimited	Yes/No	1
Colum	DoorNexSentry_bVIPBldgModeClosed	Yes/No	1
Colum	DoorNexSentry_lVIPTimegroupID	Number	4
Colum	DoorNexSentry_bSCRDRReaderEnabl	Number	1
Colum	DoorNexSentry_nForwardDigitCode	Yes/No	1
Colum	DoorNexSentry_bReadRange	Number	1
Colum	DoorNexSentry_bNumberVerifyReads	Number	1
Colum	DoorNexSentry_lVerifyTimeWindow	Number	4
Colum	DoorNexSentry_lBeeperOnDuration	Number	4
Colum	DoorNexSentry_lBeeperOffDuration	Number	4
Colum	DoorNexSentry_lBeeperOnOffDuration	Number	4
Colum	DoorNexSentry_lRedLEDOnDuration	Number	4
Colum	DoorNexSentry_lRedLEDOffDuration	Number	4

Objec	Name	Field Type	Si
Colum	DoorNexSentry_lRedLEDOnOffDuratio	Number	4
Colum	DoorNexSentry_lGreenLEDOnDuratio	Number	4
Colum	DoorNexSentry_lGreenLEDOffDuratio	Number	4
Colum	DoorNexSentry_lGreenLEDOnOffDura	Number	4
Colum	DoorNexSentry_lACUPointID	Number	4
Table	tblEmployeeCredentials		
Colum	EmployeeCredentials_lEmployeeID	Number	4
Colum	EmployeeCredentials_nCredentialID	Number	2
Table	tblFacilityCodes		
Colum	FacilityCodes_nFacilityCodeID	Number	2
Colum	FacilityCodes_sDescription	Text	30
Colum	FacilityCodes_sFacilityCode	Text	4
Table	tblFormNames		
Colum	FormNames_sFormName	Text	20
Colum	FormNames_sDescription	Text	30
Table	tblHolidays		
Colum	Holidays_dHoliday	Date/Time	8
Colum	Holidays_sDescription	Text	30
Table	tblInputs		
Colum	Inputs_lPointID	Number	4
Colum	Inputs_nType	Number	2
Colum	Inputs_nActionID	Number	2
Colum	Inputs_lACUPointID	Number	4
Table	tblInstructions		
Colum	Instructions_lInstructionID	Number	4
Colum	Instructions_sDescription	Text	30
Colum	Instructions_sInstruction	Text	25
Table	tblInternalAccessCodes		
Colum	InternalAccessCodes_lPointID	Number	4
Colum	InternalAccessCodes_nSystemCode	Number	2
Colum	InternalAccessCodes_nACUCode	Number	2
Colum	InternalAccessCodes_bIsAvailable	Yes/No	1
Colum	InternalAccessCodes_bSensorNumber	Number	1
Colum	InternalAccessCodes_nTimeGroup	Number	4
Table	tblMapData		

Objec	Name	Field Type	Si
Colum	MapData_lMapDataID	Number	4
Colum	MapData_bBlob	OLE Object	-
Colum	MapData_lBlobSize	Number	4
Table	tblMaps		
Colum	Maps_lMapID	Number	4
Colum	Maps_sMapDescription	Text	30
Table	tblMapUnits		
Colum	MapUnits_lMapID	Number	4
Colum	MapUnits_lPointID	Number	4
Colum	MapUnits_nXCoord	Number	2
Colum	MapUnits_nYCoord	Number	2
Colum	MapUnits_bLockState	Yes/No	1
Table	tblOperatorSecurity		
Colum	OperatorSecurity_bLoginID	Number	1
Colum	OperatorSecurity_sDescription	Text	30
Colum	OperatorSecurity_sLoginName	Text	20
Colum	OperatorSecurity_sPassword	Text	20
Colum	OperatorSecurity_bSecurityLevel	Number	1
Table	tblOutputs		
Colum	Outputs_lPointID	Number	4
Colum	Outputs_lACUPointID	Number	4
Table	tblPeople		
Colum	People_lEmployeeID	Number	4
Colum	People_sFirstName	Text	20
Colum	People_sMiddleName	Text	20
Colum	People_sLastName	Text	20
Colum	People_bVisitor	Yes/No	1
Colum	People_dStartDate	Date/Time	8
Colum	People_dStopDate	Date/Time	8
Colum	People_bTrace	Yes/No	1
Colum	People_bPriviledged	Yes/No	1
Colum	People_sAddress1	Text	30
Colum	People_sAddress2	Text	30
Colum	People_sAddress3	Text	30
Colum	People_nUser1	Number	2
Colum	People_nUser2	Number	2
Colum	People_nUser3	Number	2
Colum	People_nUser4	Number	2

Objec	Name	Field Type	Si
Colum	People_nUser5	Number	2
Colum	People_nUser6	Number	2
Colum	People_sUser7	Text	40
Colum	People_sUser8	Text	40
Colum	People_sUser9	Text	40
Colum	People_sUser10	Text	40
Colum	People_sUser11	Text	40
Colum	People_sUser12	Text	40
Colum	People_sUser13	Text	40
Colum	People_sUser14	Text	40
Colum	People_nAccessCode	Number	2
Table	tblPoints		
Colum	Points_lPointID	Number	4
Colum	Points_bComputer	Number	1
Colum	Points_nPoller	Number	2
Colum	Points_nAddress	Number	2
Colum	Points_nSubAddress	Number	2
Colum	Points_nSensor	Number	2
Colum	Points_nContact	Number	2
Colum	Points_sDescription	Text	30
Colum	Points_bShunted	Yes/No	1
Colum	Points_bPointClass	Number	1
Colum	Points_nTimegroupID	Number	4
Colum	Points_lInstruction	Number	4
Table	tblPollers		
Colum	Pollers_lPointID	Number	4
Colum	Pollers_bType	Number	1
Colum	Pollers_sPort	Text	20
Colum	Pollers_lBaud	Number	4
Colum	Pollers_bDataBits	Number	1
Colum	Pollers_bStopBits	Number	1
Colum	Pollers_bParity	Number	1
Colum	Pollers_bWaitTime	Number	1
Colum	Pollers_bRetryACUTime	Number	1
Table	tblSecurityLevelDescriptions		
Colum	SecurityLevelDescriptions_bSecurityLe	Number	1
Colum	SecurityLevelDescriptions_sDescriptio	Text	30
Colum	SecurityLevelDescriptions_lGrainColle	Number	4
Colum	SecurityLevelDescriptions_lGrainColle	Number	4
Colum	SecurityLevelDescriptions_lGrainColle	Number	4

Objec	Name	Field Type	Si
Colum	SecurityLevelDescriptions_lGrainColle	Number	4
Table	tblSecurityLevels		
Colum	SecurityLevels_bSecurityLevel	Number	1
Colum	SecurityLevels_nDialogID	Number	2
Colum	SecurityLevels_bAdminister	Yes/No	1
Table	tblSiteCodes		
Colum	SiteCodes_nSiteCodeID	Number	2
Colum	SiteCodes_sDescription	Text	30
Colum	SiteCodes_sSiteCode	Text	4
Table	tblSoundData		
Colum	SoundData_lSoundID	Number	4
Colum	SoundData_bBlob	OLE Object	-
Colum	SoundData_lBlobSize	Number	4
Table	tblSounds		
Colum	Sounds_lSoundID	Number	4
Colum	Sounds_sDescription	Text	30
Table	tblSystem		
Colum	System_sCompanyName	Text	30
Colum	System_bDownloadACUOnDiscrepanc	Yes/No	1
Colum	System_tDownloadACUAt	Date/Time	8
Colum	System_bPrintFormFeedOnAlarm	Yes/No	1
Colum	System_nMonitorMessageCount	Number	2
Colum	System_bSystemDataDirty	Yes/No	1
Colum	System_bKeyDataDirty	Yes/No	1
Colum	System_sReportPrinter	Text	50
Table	tblTimecodes		
Colum	Timecodes_lTimecodeID	Number	4
Colum	Timecodes_sDescription	Text	30
Colum	Timecodes_tStartTime	Date/Time	8
Colum	Timecodes_tEndTime	Date/Time	8
Colum	Timecodes_bSunday	Yes/No	1
Colum	Timecodes_bMonday	Yes/No	1
Colum	Timecodes_bTuesday	Yes/No	1
Colum	Timecodes_bWednesday	Yes/No	1
Colum	Timecodes_bThursday	Yes/No	1
Colum	Timecodes_bFriday	Yes/No	1
Colum	Timecodes_bSaturday	Yes/No	1

Objec	Name	Field Type	Si
Colum	Timecodes_bHoliday	Yes/No	1
Table	tblTimegroups		
Colum	Timegroups_lTimegroupID	Number	4
Colum	Timegroups_sDescription	Text	30
Colum	Timegroups_nTimecodeID1	Number	4
Colum	Timegroups_nTimecodeID2	Number	4
Colum	Timegroups_nTimecodeID3	Number	4
Colum	Timegroups_nTimecodeID4	Number	4
Table	tblTransactionLog		
Colum	TransactionLog_lTransactionID	Number	4
Colum	TransactionLog_lPointID	Number	4
Colum	TransactionLog_lEmployeeID	Number	4
Colum	TransactionLog_nCredentialID	Number	2
Colum	TransactionLog_dTransactionLogDate	Date/Time	8
Colum	TransactionLog_tTime	Date/Time	8
Colum	TransactionLog_nTransactionType	Number	2
Colum	TransactionLog_bPriority	Number	1
Colum	TransactionLog_dAcknowledgeDate	Date/Time	8
Colum	TransactionLog_tAcknowledgeTime	Date/Time	8
Colum	TransactionLog_bACUUserID	Number	1
Colum	TransactionLog_bLoginID	Number	1
Colum	TransactionLog_sAlarmRemarks	Text	25
Colum	TransactionLog_bAlarmStatus	Number	1
Colum	TransactionLog_nAlarmResponseID	Number	2
Table	tblTransactionType		
Colum	TransactionType_nTransactionType	Number	2
Colum	TransactionType_sDescription	Text	30
Colum	TransactionType_bFgRedColor	Number	1
Colum	TransactionType_bFgGreenColor	Number	1
Colum	TransactionType_bFgBlueColor	Number	1
Colum	TransactionType_bPriority	Number	1
Colum	TransactionType_bSendToPrinter	Yes/No	1
Colum	TransactionType_bLogToDisk	Yes/No	1
Colum	TransactionType_bAlertOperator	Yes/No	1
Colum	TransactionType_bAlertContinuous	Yes/No	1
Colum	TransactionType_bEnableSound	Yes/No	1
Colum	TransactionType_nIconIndex	Number	2
Colum	TransactionType_lInstruction	Number	4
Colum	TransactionType_lSound	Number	4

Objec	Name	Field Type	Si
Table	tblUser1		
Colum	User1_nUserID	Number	2
Colum	User1_nPositionIndex	Number	2
Colum	User1_sDescription	Text	30
Table	tblUser2		
Colum	User2_nUserID	Number	2
Colum	User2_nPositionIndex	Number	2
Colum	User2_sDescription	Text	30
Table	tblUser3		
Colum	User3_nUserID	Number	2
Colum	User3_nPositionIndex	Number	2
Colum	User3_sDescription	Text	30
Table	tblUser4		
Colum	User4_nUserID	Number	2
Colum	User4_nPositionIndex	Number	2
Colum	User4_sDescription	Text	30
Table	tblUser5		
Colum	User5_nUserID	Number	2
Colum	User5_nPositionIndex	Number	2
Colum	User5_sDescription	Text	30
Table	tblUser6		
Colum	User6_nUserID	Number	2
Colum	User6_nPositionIndex	Number	2
Colum	User6_sDescription	Text	30
Table	tblUserFieldNames		
Colum	User_nUserFieldID	Number	1
Colum	User_sUserFieldPrompt	Text	10
Colum	User_sUserHelpText	Text	80
Table	tblZonePoints		
Colum	ZonePoints_nZoneID	Number	2
Colum	ZonePoints_ulPointID	Number	4
Table	tblZones		
Colum	Zones_nZoneID	Number	2
Colum	Zones_sDescription	Text	30

Glossary

ABA card

See *American Banking Association (ABA) card.*

access code

The number that defines where and when individual cardholders will have access.

access control unit (ACU)

Access Control Units (ACUs) are devices which sense and react to inputs from the secured environment. ACUs control door status (open or closed), in conjunction with the host or local computer.

acknowledge alarm

The action an operator takes to respond to an alarm message in the Alarm Servicing dialog box.

action

The defined way in which an ACU will respond to an event.

ACU

See *access control unit (ACU).*

ACU transactions

All of the security events occurring on the ACU. This is synonymous with the term “Transaction” in the NexSentry Manager.

additional look-up

User defined fields that a system operator can use to store additional information about cardholders.

additional text fields

User defined fields that a system operator can use to store information about cardholders. The additional text fields allow system operators more flexibility in filtering and sorting cardholders.

alarm handling

There are several ways for an operator to respond to an alarm: Silence the Alarm, Clear the Alarm, or Mark the Alarm as read.

alarm

User defined Outputs, either messages to the system operators or to others (police or fire departments) to notify of abnormal conditions.

American Banking Association (ABA) card

An industry standard magnetic stripe card.

annunciator

An optional unit that connects to the ACU that provides for an expanded response function such as alarm sirens, blowers, cameras, lights, pumps, etc.

anti-passback

A control measure that prevents a cardholder from re-using a door prior to using an exit through another door. This prevents an unsecure practice of a cardholder going through a door, and then handing back his or her card to someone else to use. This control works on the ACU level and is not managed by the NexSentry Manager.

archive transactions

A process of transferring transaction log data from the Database to a storage disk, either the hard drive or a floppy drive. This allows the user to remove transactions but to save them for historical reference.

AT&T smart card

A type of keycard that may be used with a smart card reader.

Building Mode

A control method that allows the system user to define the overall access to a building or sector. The three building modes are Open, Limited, and Closed.

cardholder

Cardholders are individuals who have a security card and access to the controlled areas.

child window

A Windows NT term that refers to a second level screen. In the NexSentry Manager, the Monitor window or the Status window would be considered child windows

client

A computer that requests the service of another computer. A workstation requesting the contents of a file from a file server is a client of the file server.

credentials

In the NexSentry Manager, the specific keycard information for each cardholder, including card type, number, PIN and Facility Code.

data entry dialog box

The screen or window that allows the system user to enter and save information.

Database Management System (DBMS)

A complex set of software instructions that controls the organization, storage and retrieval of data (fields, records and files) in a database. It also controls the security and integrity of the database. The DBMS accepts requests for data from the application program and instructs the operating system to transfer the appropriate data.

DBMS

See *Database Management System (DBMS).*

digital key reader (DKR)

A proximity sensor connected to an ACU that reads digital cards used with the system.

digital card

A credit-card-like card with encrypted data that is read by digital or proximity readers.

door switch

A monitoring device that detects if the door is open or closed.

facility code

Unique identification number assigned to a facility, which allows additional access control. Facility codes are available only for 1030 and 1040 key cards.

holiday

The user defined days in which the controlled environment can be handled differently for a holiday. System operators can define time groups to allow access during days defined as a holiday.

instruction

A user defined message that displays to the operator when a defined event occurs.

keypad

An optional device that allows a cardholder to enter access information by pressing keys most commonly as a PIN.

LAN

See *Local Area Network.*

latched contact

A relay (output contact) which, once it goes active as a result of an input, stays active until an operator silences or clears it.

local area network (LAN)

A group of computers and other devices usually dispersed over a relatively limited area and connected by a communications link that enables any device to interact with any other on the network.

magnetic stripe reader (MSR)

An access device that reads magnetic stripe cards.

map

In the NexSentry Manager, Maps are a way to graphically represent the secured environment. The Maps will allow you to monitor, check system status, manually unlock or lock doors, etc. just as you would do from the Monitor or System status window.

MDI

See *Multiple Document Interface.*

MI

See *monitored inputs.*

Microsoft Windows NT

The computer operating system required to use the NexSentry Manager. You must use Windows NT version 4.00 or later. It is Microsoft's 32 bit operating system which features true multi-tasking, built in networking, security, and memory protection.

monitor points

General purpose switches that detect and provide information to the system. These can be sensors that detect when a window is broken, unauthorized movement, temperature, or other defined conditions.

monitored inputs (MI)

General purpose switch that is activated by a condition such as a broken window, rise in temperature, movement, or liquid level.

MSM

See multiple switch monitor.

MSR

See *magnetic stripe reader (MSR).*

multiple switch monitor

A link between monitor points and the ACU which allows for up to four monitor points.

network node

One of the software-addressable components on a NexSentry system, such as a MIRO, DKR, a VIP-2 Keypad or an ACU.

ODBC

See *Open Database Connectivity.*

Open Database Connectivity (ODBC)

An industry standard Database Management system designed by Microsoft. In Windows NT, the NexSentry Manager automatically configures this setting in the Control Panel during installation. See *Database Management System (DBMS).*

parent window

A Windows NT term that refers to a first level screen. In the NexSentry Manager, the Main window would be considered a parent window.

personal identification number (PIN)

Unique four- to eight-digit numbers that cardholders enter into keypads (VIPs or Magnetic Stripe Key Readers for example) and are used either in combination with card readers or alone to grant access.

personnel

In the NexSentry Manager, personnel refers to the portion of the Database where you enter information about the cardholders.

PIN

See *personal identification number (PIN).*

poller

A NexSentry Manager device that controls communications with devices in the access control system.

pollers data entry dialog box

The window or screen in which the system operator will define the poller based on the information provided by the installer and contained in the data input forms.

privileged access

An access that entitles an individual to enter a building/sector when it is in closed mode. It is usually part of an access code with 24-hour access. Not available when building/sector modes are not used.

record selection dialog box

The dialog box that displays the records of a certain type of hardware or system data, in which you can select individual entries to edit or add new entries.

relay output (RO)

Works with an Monitored Input as a response to a condition, such as sounding an alarm for a broken window.

report

The NexSentry Manager has pre-define report formats depending on the current window or dialog box.

request-to-exit (REX)

A special monitor that is usually mounted inside a door, such as an electric eye or a pressure pad, that allows cardholders to unlock a door when exiting a secured door.

REX

See *request-to-exit.*

RO

See r*elay outputs.*

S-Net device

Security device within the security network (SNET), such as ACUs, card readers, VIPs, etc.

SCR

See *smartcard readers.*

security electronics extended protocol

A proprietary communications protocol designed by Westinghouse Security Electronics.

Security Management System

A computer networking system like the NexSentry Manager that communicates with individual access control units.

security level

Security levels determine which users have access to different portions of the NexSentry Manager software. You can define the number of security levels and the limit access to various NexSentry Manager functions based on your needs.

security network (SNET)

Comprised of all of the hardware components of the security system, such as ACUs, Card Readers, VIPs, etc.

SEEP

See *security electronics extended protocol.*

server

A computer which, by means of network connections, carries out parts of a computing task on behalf of one or more remote computers. The computer where the NexSentry Manager Database is located is the NexSentry Server.

shunt

A command issued to ignore a device or its messages. Example: Ignore messages from an open door when workers are moving furniture in and out of a building. *See unshunt.*

SI

See *sensor interface.*

smartcard reader (SCR)

A security hardware device that uses radio signals to read the unique number encoded on an AT&T Smart Card.

SNET

See *security network.*

system administration

Consists of all the tasks responsible for creating, revising and maintaining the entire NexSentry Manager Database.

system administrator

Person responsible for managing the NexSentry Database. This person usually manages all of the system operators as well.

system user

An operator with a password who is authorized to use the NexSentry Manager.

time code

A specific format that tells the ACU days and times for specific actions or access.

traced access

An additonal transaction controlled by a flag in the cardholder's record. See also *access codes.*

transaction

Individual "events" that occur in the secured environment. Transactions are displayed in the Monitor Window in real time and stored in the Transaction Log. These events are all of the normal and abnormal occurrences within the security system.

user defined field

Additional fields that a system operator can use to store information about cardholders that is unique to the system.

unshunt

A command to reverse the Shunt command. This is given to restore communication between the NexSentry Manager, the ACU and the particular device that was "shunted." *See shunt.*

VIP

A type of keypad that is used on the NexSentry Manager. *See keypad.*

visitor access

See *access codes.*

Windows NT

See *Microsoft Windows NT.*

zone

A zone is any logical grouping of hardware elements that is determined by the NexSentry Manager System Administrator. A zone does not have to be solely geographic, but can include like items, such as all exterior doors.

INDEX

A

Access Codes, 4-2
Access Control, vii
Access Control Unit, 3-5
Action Groups, 2-23
Actions, 2-21
ACU, 1-1, 3-5
    Addressing, 2-9, 3-5
    Data, 3-7
    Users, 2-8
ACU Users, 2-8
Add From, 3-4, 3-8
Alarm Response, 2-12
Alarms
    Acknowledging, 5-8
    Silencing, 5-8
    Viewing, 5-8
Archiving, 5-6
Assumptions, 1-2
Audit Trail
    Archiving, 2-14, 5-6
    Viewing, 2-13
AutoFit, 5-13

B

Backing Up, 5-15
Baud Rate, ACU default, 3-6

C

Cardholder, 1-1
    Adding, 4-4
    Data, 1-12
    Editing, 4-4
    Viewing, 4-5

D

Database
    Browsing, 1-13, 3-2
    Using, 1-13
default, log-on name, 1-4
default, password, 1-5
Dialog Box
    Access Codes, 4-2
    Action Groups, 2-23
    Actions, 2-21
    ACU, 3-7
    ACU User, 2-8
    Alarm Response, 2-12
    Archive, 5-7
    Cardholder, 4-4
    Door, 3-9
    Input, 3-11
    Instructions, 3-15
    Outputs, 3-13
    Pollers, 3-3
    properties, 1-14
    System Defaults, 2-27
    System User, 2-6
    Time Groups, 2-19
    Transactions Type, 2-10
    User Defined Fields, 2-14
    Zones, 3-16
Door, 3-9

F

Facility Codes, 2-16
Facility Data, 1-1, 1-11
Filter, 1-16

H

Hardware, 1-1, 1-11
Holidays, 2-20
Hyperterminal
    Using to Address ACU, 3-5

I

Input Forms, 1-12
Inputs, 3-11
Installation, 1-4, 2-2
Instructions, 3-15

IP Address, 6-2

K

Key Terms, 1-1, 2-1, 3-1, 4-1, 5-1

L

log-on name, default, 1-4

M

Main Menu, 1-9
Main Program window, 1-9
Maps
    Background File, 3-17
    Create, 3-17
    Droping and Dragging Icons, 3-18
    List of Defined, 2-25
    Locking Icons, 3-18
    Map Tool, 3-17
    Naming and Renaming, 3-18
    Viewing, 5-14
Monitor
    Using, 5-2
    Viewing Recent Transactions, 5-3
    Window, 5-2

N

NexSentry Manager
    System Administration, 2-2

O

Online Help, 1-10
Operators, 1-11
Outputs, 3-13

P

password,default, 1-5
Passwords, 2-7
Pollers, 1-1, 3-3
Preface, vii
Print, 1-15
Printer
    Log Printer, 2-27
Proximity Reader, 3-10

R

REX, 3-10

S

Security Levels, 2-4
Sort, 1-16
    Examples, 1-16
Sounds, 2-26
Status Bar, 1-9
Status Menu
    Activating, 5-11
    Options and Descriptions, 5-11
Status Window, 5-10
    Filtering, 5-10
System, 1-2
System Administrator Data, 1-1
System Defaults, 2-27
System Requirements, 1-2
System Status, 5-10
System User, 2-6

T

Time Codes, 2-17
Time Groups, 2-19, 3-10
Toolbar, 1-9
Transaction
    Log, 2-10
    Type, 2-10
Transaction Log
    Viewing, 5-5
Transactions
    Archiving, 5-6
    Changing Defaults, 5-5

Sort, 5-3
Viewing or Editing, 5-5

U

User Defined Fields, 2-14
Additional Look-Up Fields, 2-14
Additonal Text Fields, 2-14
Using this Guide, ix

V

VIP, 3-10

W

WAV File, 2-26
Window
Browse Database, 1-13

Z

Zones, 3-16